

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-214233

(43) 公開日 平成10年(1998) 8月11日

(51) Int.Cl. ⁸	識別記号	FI	
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
G 0 9 C 1/00	6 3 0	G 0 9 C 1/00	6 3 0 A
	6 6 0		6 6 0 D
			6 6 0 A
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
審査請求 未請求 請求項の数25 OL (全 29 頁) 最終頁に続く			

(21) 出願番号 特願平9-97583

(22) 出願日 平成9年(1997) 4月15日

(31) 優先権主張番号 特願平8-92516

(32) 優先日 平8(1996) 4月15日

(33) 優先権主張国 日本 (JP)

(31) 優先権主張番号 特願平8-320291

(32) 優先日 平8(1996) 11月29日

(33) 優先権主張国 日本 (JP)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 清水 秀夫

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 遠藤 直樹

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 才所 敏明

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74) 代理人 弁理士 鈴江 武彦 (外6名)

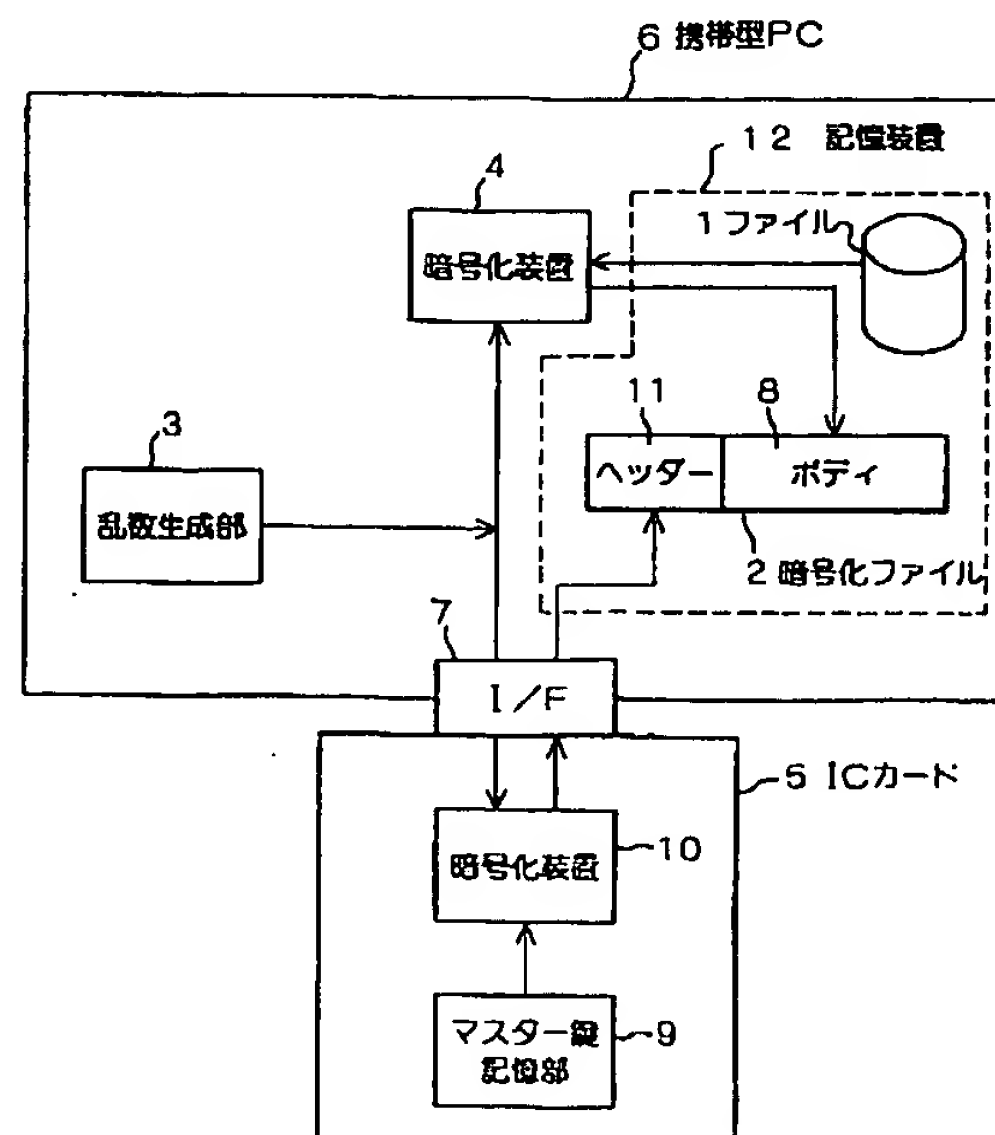
最終頁に続く

(54) 【発明の名称】 情報処理装置、情報処理システム、情報処理方法、プログラム記憶装置、及び鍵の判定方法及び判定装置

(57) 【要約】

【課題】 たとえ装置が盗難されたり分解されたりしても、内部に記憶された機械情報を保護することができる情報処理システムを提供する。

【解決手段】 携帯型PC 6と、この携帯型PC 6とは別体で構成されており、かつ携帯型PC 6と信号の受渡しが可能なICカード 5とを具備する情報処理システムであって、携帯型PC 6は、一時鍵を生成するための乱数生成部 3と、一時鍵を用いてデータを暗号化してボディ部 8を生成するための暗号化装置 4とを備え、ICカード 5は、マスター鍵を記憶するためのマスター鍵記憶部 9と、マスター鍵を用いて一時鍵を暗号化してヘッダー部 11を生成するための暗号化装置 10とを備え、携帯型PC 6は、ボディ部 8と、ヘッダー部 11とを合成して暗号化ファイル 2として記憶するための記憶装置 12をさらに具備する。



BEST AVAILABLE COPY (JP5010)

BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 第1の情報処理装置と、この第1の情報処理装置とは別体で構成されており、かつ前記第1の情報処理装置と信号の受渡しが可能な第2の情報処理装置とを具備する情報処理システムであって、

前記第1の情報処理装置は、

第1の鍵を生成するための第1鍵生成手段と、

この第1鍵生成手段によって生成された前記第1の鍵を用いてデータを暗号化して第1暗号情報を生成するための第1暗号化手段とを備え、

前記第2の情報処理装置は、

第2の鍵を記憶するための第2鍵記憶手段と、

この第2鍵記憶手段に記憶された前記第2の鍵を用いて前記第1の鍵を暗号化して第2暗号情報を生成するための第2暗号化手段と、を備え、

前記第1の情報処理装置は、前記第1暗号化手段によって生成された前記第1暗号情報と、前記第2暗号化手段によって生成された前記第2暗号情報とを関連付けて記憶するための関連付け記憶手段をさらに具備することを特徴とする情報処理システム。

【請求項2】 前記第1の暗号化手段は、前記第1暗号化情報を生成した後に、前記データを削除する手段を有する請求項1記載の情報処理システム。

【請求項3】 第1の情報処理装置と、この第1の情報処理装置とは別体で構成されており、かつ前記第1の情報処理装置と信号の受渡しが可能な第2の情報処理装置とを具備する情報処理システムであって、

前記第1の情報処理装置は、

第1の鍵によりデータを暗号化した第1暗号情報と、第2の鍵により第1の鍵を暗号化した第2暗号情報とを関連付けて記憶するための関連付け記憶手段を備え、

前記第2の情報処理装置は、

第2の鍵を記憶するための第2鍵記憶手段と、

この第2鍵記憶手段に記憶された前記第2の鍵により、前記関連付け記憶手段から読み出された前記第2暗号情報を復号して前記第1の鍵を取出すための第1復号手段と、を備え、

前記第1の情報処理装置は、前記第1復号手段によって取り出された前記第1の鍵により、前記関連付け記憶手段に記憶された前記第1暗号情報を復号して前記データを取得するための第2復号手段をさらに具備することを特徴とする情報処理システム。

【請求項4】 第1の鍵を生成するための第1鍵生成手段と、

この第1鍵生成手段によって生成された前記第1の鍵によりデータを暗号化するための暗号化手段と、

前記第1鍵生成手段によって生成された前記第1の鍵を外部情報処理装置へ出力し、該外部情報処理装置内で当該装置内に記憶されている第2の鍵により暗号化された前記第1の鍵を入力するための入力手段と、

この入力手段を介して入力される前記暗号化された第1の鍵と、前記暗号化手段によって暗号化された前記データとを関連付けて記憶するための記憶手段と、を具備することを特徴とする情報処理装置。

【請求項5】 前記暗号化手段は、前記データを暗号化した後に、当該データを削除する手段を有することを特徴とする請求項4記載の情報処理装置。

【請求項6】 第1の鍵によりデータを暗号化した第1暗号情報と、第2の鍵により前記第1の鍵を暗号化した第2暗号情報とを記憶するための記憶手段と、

この記憶手段に記憶されている前記第2の暗号情報を外部情報処理装置へ出力し、該外部情報処理装置内で当該外部情報処理装置内に記憶されている第2の鍵により前記第2暗号情報を復号して得られる復号された第1の鍵を入力するための入力手段と、

この入力手段を介して入力された前記復号された第1の鍵により前記第1暗号情報を復号して前記データを取得するための復号化手段とを具備することを特徴とする情報処理装置。

【請求項7】 第2の鍵を記憶するための記憶手段と、第1の鍵を生成し、この第1の鍵によりデータを暗号化する外部情報処理装置から、前記第1の鍵を入力するための入力手段と、

前記記憶手段に記憶されている前記第2の鍵によって、前記入力手段を介して入力される前記第1の鍵を暗号化するための暗号化手段と、

前記外部情報処理装置において、この暗号化手段によって暗号化された第1の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第1の鍵を前記外部情報処理装置へ出力するための出力手段と、を具備することを特徴とする情報処理装置。

【請求項8】 第2の鍵を記憶するための記憶手段と、第1の鍵によりデータを暗号化して得られる第1暗号情報と、前記記憶手段に記憶された前記第2の鍵により、前記第1の鍵を暗号化して得られる第2暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から、前記第2暗号情報を入力するための入力手段と、

この入力手段を介して入力された前記第2暗号情報を前記第2の鍵により復号して前記第1の鍵を取出すための復号手段と、

前記外部情報処理装置において、前記復号手段により取り出された前記第1の鍵により前記第1暗号情報を復号して前記データを取得するために、前記取り出された第1の鍵を前記外部情報処理装置へ出力するための出力手段と、を具備することを特徴とする情報処理装置。

【請求項9】 第1の情報処理装置内で第1の鍵を生成する第1鍵生成工程と、

生成された第1の鍵を用いてデータを暗号化して第1暗号情報を生成する第1暗号情報生成工程と、

生成された第1の鍵を、前記第1の情報処理装置とは別

3

体で構成され、第2の鍵を記憶している第2の情報処理装置へ出力する出力工程と、
前記第2の情報処理装置内で前記第2の鍵を用いて前記第1の鍵を暗号化して第2暗号情報を生成する第2暗号情報生成工程と、
生成された第2暗号情報を前記第1の情報処理装置へ出力する出力工程と、
前記第1情報処理装置内で前記第1暗号情報と前記第2暗号情報とを関連付けて記憶する記憶工程と、を具備することを特徴とする情報処理方法。

【請求項10】 第1の鍵によりデータを暗号化して得られた第1暗号情報と、第2の鍵により前記第1の鍵を暗号化して得られた第2暗号情報とが関連付けて記憶されている第1の情報処理装置内から、前記第2暗号情報を、当該第1の情報処理装置とは別体で構成された第2の情報処理装置へ出力する出力工程と、
前記第2の情報処理装置内に予め記憶されている前記第2の鍵により、前記第2暗号情報を復号して前記第1の鍵を取り出す第1鍵取り出し工程と、
取り出された第1の鍵を前記第1の情報処理装置へ出力する出力工程と、
前記第1の情報処理装置において、当該第1の鍵により前記第1暗号情報を復号して前記データを得るデータ取得工程と、を具備することを特徴とする情報処理方法。

【請求項11】 第1の鍵を生成する第1鍵生成工程と、
生成された第1の鍵によりデータを暗号化する暗号化工程と、
生成された第1の鍵を外部情報処理装置へ出力する出力工程と、
当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第2の鍵により暗号化された第1の鍵を入力する入力工程と、
入力された前記暗号化された第1の鍵と、前記第1の鍵により暗号化されたデータとを関連付けて記憶する記憶工程と、を具備することを特徴とする情報処理方法。

【請求項12】 第1の鍵によりデータを暗号化して記憶された第1暗号情報と、第2の鍵により第1の鍵を暗号化して記憶された第2暗号情報のうち、前記第2の暗号情報を外部情報処理装置へ出力する出力工程と、
該外部情報処理装置内で当該外部情報処理装置内に記憶されている前記第2の鍵により前記第2暗号情報を復号して得られた前記第1の鍵を入力する入力工程と、
入力された前記第1の鍵により前記第1暗号情報を復号して前記データを取り出す取り出し工程と、を具備することを特徴とする情報処理方法。

【請求項13】 生成された第1の鍵によりデータを暗号化する外部情報処理装置から前記第1の鍵を入力する入力工程と、
予め記憶されている第2の鍵により入力された前記第1

4

の鍵を暗号化する暗号化工程と、
前記外部情報処理装置において、この暗号化された第1の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第1の鍵を前記外部情報処理装置へ出力する出力工程と、を具備することを特徴とする情報処理方法。

【請求項14】 第1の鍵によりデータを暗号化して得られた第1暗号情報と、第2の鍵により第1の鍵を暗号化して得られた第2暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から前記第2暗号情報を入力する入力工程と、

予め記憶している第2の鍵により前記第2暗号情報を復号して前記第1の鍵を取り出す取り出し工程と、
前記外部情報処理装置において、取り出された前記第1の鍵により前記第1暗号情報を復号して前記データを得るために、復号により取り出された前記第1の鍵を前記外部情報処理装置へ出力する出力工程と、を具備することを特徴とする情報処理方法。

【請求項15】 暗号化処理を実行する方法ステップを遂行するために、マシンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記方法ステップは、
第1の鍵を生成する第1鍵生成ステップと、
生成された第1の鍵によりデータを暗号化する暗号化ステップと、
生成された第1の鍵を外部情報処理装置へ出力する出力ステップと、
当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第2の鍵により暗号化された第1の鍵を入力する入力ステップと、
入力された前記暗号化された第1の鍵と、前記第1の鍵により暗号化されたデータとを関連付けて記憶する記憶ステップと、を具備することを特徴とするプログラム記憶装置。

【請求項16】 暗号化処理を実行する方法ステップを遂行するために、マシンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、
前記方法ステップは、
第1の鍵によりデータを暗号化して記憶された第1暗号情報と、第2の鍵により第1の鍵を暗号化して記憶された第2暗号情報のうち、前記第2の暗号情報を外部情報処理装置へ出力する出力ステップと、
該外部情報処理装置内で当該外部情報処理装置内に記憶されている前記第2の鍵により前記第2暗号情報を復号して得られた前記第1の鍵を入力する入力ステップと、
入力された前記第1の鍵により前記第1暗号情報を復号して前記データを取り出す取り出しステップと、を具備することを特徴とするプログラム記憶装置。

【請求項17】 送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵でそれぞれ暗号化あるい

は復号して送信し、受信側で、前記複数の第2の鍵の中から受信側で有している特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定方法において、

前記第1の鍵を前記複数の第2の鍵でそれぞれ暗号化あるいは復号化して得られた第1データを入力する入力工程と、

前記第1データの中で前記特定の第2の鍵で暗号化あるいは復号化された特定の第1データと所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力工程と、
10 入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出工程と、

抽出された前記特定の第2の鍵を出力する出力工程と、を具備することを特徴とする鍵の判定方法。

【請求項18】 送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵の中の特定の第2の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第2の鍵の中から前記特定の第2の鍵を抽出するための鍵の判定方法において、

前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する入力工程と、
前記第1データと所定の処理を行なうことにより、前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力工程と、

入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出工程と、

抽出された前記特定の第2の鍵を出力する出力工程と、を具備することを特徴とする鍵の判定方法。

【請求項19】 送信側で、データを暗号化するのに用いた第1の鍵を送信側及び受信側が共に有している複数の第2の鍵の中から、特定の第2の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定方法であって、

前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する入力工程と、

前記第1データの中と所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力工程と、

入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出工程と、

抽出された前記特定の第2の鍵を出力する出力工程と、を具備することを特徴とする鍵の判定方法。

【請求項20】 送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第2の鍵の中

から受信側で有している特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定装置であって、

前記第1の鍵を前記複数の第2の鍵でそれぞれ暗号化あるいは復号化して得られた第1データを入力する第1入力手段と、

この第1入力手段によって入力された前記第1データの中で、前記特定の第2の鍵で暗号化あるいは復号化された特定の第1データと所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する第2入力手段と、

この第1入力手段によって入力された前記第1データと、前記第2入力手段によって入力された前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出手段と、

この抽出手段によって抽出された前記特定の第2の鍵を出力する出力手段と、を具備することを特徴とする鍵の判定装置。

【請求項21】 送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵の中の特定の第2の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第2の鍵の中から前記特定の第2の鍵を抽出するための鍵の判定装置であって、

前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する第1入力手段と、
この第1入力手段によって入力された前記第1データと所定の処理を行なうことにより、前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する第2入力手段と、

この第2入力手段によって入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出手段と、
この抽出手段によって抽出された前記特定の第2の鍵を出力する出力手段と、を具備することを特徴とする鍵の判定装置。

【請求項22】 送信側で、データを暗号化するのに用いた第1の鍵を送信側及び受信側が共に有している複数の第2の鍵の中から、特定の第2の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定装置であって、

前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する第1入力手段と、
この第1入力手段によって入力された前記第1データの中と所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する第2入力手段と、

前記第1入力手段によって入力された前記第1データと、前記第2入力手段によって入力された前記第2データとに基づいて、前記所定の処理を行なうことにより前

10

20

30

40

50

記特定の第2の鍵を抽出する抽出手段と、
この抽出手段によって抽出された前記特定の第2の鍵を
出力する出力手段と、を具備することを特徴とする鍵の
判定装置。

【請求項23】 送信側で、データを暗号化するのに用
いた第1の鍵を複数の第2の鍵でそれぞれ暗号化ある
いは復号して送信し、受信側で、前記複数の第2の鍵の中
から受信側で有している特定の第2の鍵に該当する第2
の鍵を前記複数の第2の鍵の中から抽出して鍵の判定を
行なう判定ステップを遂行するために、マシンリーダ
ブルなプログラムを記憶したプログラム記憶装置であ
って、

前記判定ステップは、

前記第1の鍵を前記複数の第2の鍵でそれぞれ暗号化あ
るいは復号化して得られた第1データを入力する入力ス
テップと、

前記第1データの中で前記特定の第2の鍵で暗号化ある
いは復号化された特定の第1データと所定の処理を行な
うことにより前記特定の第2の鍵が得られるような処理
によって処理された第2データを入力する入力ステップ
と、

入力された前記第1データと前記第2データとに基づい
て、前記所定の処理を行なうことにより前記特定の第2
の鍵を抽出する抽出ステップと、

抽出された前記特定の第2の鍵を出力する出力ステッ
プと、を具備することを特徴とするプログラム記憶装置。

【請求項24】 受信側で、データを暗号化するのに用
いた第1の鍵を複数の第2の鍵の中の特定の第2の鍵で
暗号化あるいは復号化して送信し、受信側で、前記複数
の第2の鍵の中から前記特定の第2の鍵を抽出して鍵の
判定を行なう判定ステップを遂行するために、マシン
リーダブルなプログラムを記憶したプログラム記憶装置
であって、

前記判定ステップは、

前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復
号して得られた第1データを入力する入力ステップと、
前記第1データと所定の処理を行なうことにより、前記
特定の第2の鍵が得られるような処理によって処理され
た第2データを入力する入力ステップと、

入力された前記第1データと前記第2データとに基づい
て、前記所定の処理を行なうことにより前記特定の第2
の鍵を抽出する抽出ステップと、

抽出された前記特定の第2の鍵を出力する出力ステッ
プと、を具備することを特徴とするプログラム記憶装置。

【請求項25】 送信側で、データを暗号化するのに用
いた第1の鍵を送信側及び受信側が共に有している複数
の第2の鍵の中から、特定の第2の鍵で暗号化あるいは
復号して送信し、受信側で、前記特定の第2の鍵に該当
する第2の鍵を前記複数の第2の鍵の中から抽出して鍵
の判定を行なう判定ステップを遂行するために、マシン

リーダブルなプログラムを記憶したプログラム記憶装置
であって、

前記判定ステップは、

前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復
号して得られた第1データを入力する入力ステップと、
前記第1データの中と所定の処理を行なうことにより前
記特定の第2の鍵が得られるような処理によって処理さ
れた第2データを入力する入力ステップと、

入力された前記第1データと前記第2データとに基づい
て、前記所定の処理を行なうことにより前記特定の第2
の鍵を抽出する抽出ステップと、

抽出された前記特定の第2の鍵を出力する出力ステッ
プと、を具備することを特徴とするプログラム記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は情報処理装置、情報
処理システム、情報処理方法、記録媒体（プログラム記
憶装置）、及び鍵の判定方法及び装置に関し、特に、I
Cカード等との間で信号の受け渡し可能な携帯型パー
ソナルコンピュータにおいて、ファイル暗号化システム
を備えた情報処理装置、情報処理システム、情報処理方
法、記録媒体、及び鍵の判定方法及び装置に関する。

【0002】

【従来の技術】近年、技術の進歩によりコンピュータの
小型化が進み、操作者が所望の場所に移動させて操作で
きる携帯型パーソナルコンピュータが登場している。こ
のような携帯型パーソナルコンピュータはハードディス
ク等の大容量外部記憶装置を内蔵しており、携帯型であ
っても種々のアプリケーションプログラムや作成したフ
ァイルを記憶することが可能である。

【0003】ところで、携帯型以外のコンピュータの場合
は屋内に設置される場合が多いので、コンピュータが
設置してある部屋への出入りを制限する等の方法によっ
てコンピュータの内部に格納されている機密情報を不正
な第三者から保護することが可能である。また、通信ネ
ットワークの発展により、ローカルホストからリモート
ホストの内部に侵入して不正を行なうといったことが可
能になったが、この場合でも、リモートホスト自体は物
理的に隔離された場所に配置されているのでリモートホ
スト自体に直接被害が及ぶということはない。

【0004】ところが上記した携帯型パーソナルコンピ
ュータにおいては、携帯が可能であるために、装置自体
が盗難されてその内部に格納されている機密情報が盗ま
れてしまう可能性がある。そこで、パスワードなどを用
いて、たとえ盗難されてもパスワードの保持者以外は使
用できないようにする方法が考えられる。しかしなが
ら、このような方法を用いたとしても装置自体を分解し
て内蔵されているハードディスクを取り出し、ハードデ
ィスクに格納されている機密情報入手することが可能
である。分解できないパーソナルコンピュータを製造す

ることは困難であり、仮に製造可能であったとしても、装置が大型になって携帯に適さなくなるとともに、製造コストが増大してしまうという問題が新たに発生する。

【0005】また、近年、データを複数のユーザで共有するケースが増加してきている。例えば、1台のパーソナルコンピュータを複数のユーザで共用する形態においてそのパーソナルコンピュータに内蔵されたハードディスク装置内のデータを共有する場合、あるいは各ユーザのパーソナルコンピュータをLANなどで接続し、このLANに接続された記録装置を複数のユーザで共用する形態においてこの記録装置内のデータを共有する場合などである。

【0006】従って、ユーザ個人のデータを安全に保存するだけでなく、複数のユーザで共有するデータで高い機密性を要するものについても安全性を確保する必要性が生じている。

【0007】しかし、同一データを複数のユーザ間で共有する場合、暗号鍵と復号鍵の対は、個人用に加えて、グループ用のものを用意し、同一データを、これを共有するユーザの個人用暗号鍵やグループ用暗号鍵夫々で暗号化して、同一の内容を持つ複数の暗号化データを作成し保存することになるため、鍵の種類が多くなるとともに、暗号化データの種類も多くなり、鍵情報と暗号化データの管理が困難になるという問題点があった。また、従来は、間違った鍵で暗号化データを復号したために、内容を破壊してしまうようなトラブルも生じる可能性があった。

【0008】

【発明が解決しようとする課題】上記したように、携帯型パーソナルコンピュータの出現によって利便性が向上したが、携帯型であるがために装置自体が盗難されて内部に格納されている機密情報が不正な第三者に知られてしまうという問題がある。また、パスワード等により機密情報へのアクセスを制限した場合でも、装置自体を分解して内蔵されているハードディスクを取り出し、ハードディスクに格納されている機密情報を入手することが可能であるという問題がある。

【0009】また、個人やグループが共有するデータを、各々のマスタ鍵により復号可能な形で暗号化し保存するためには、各々のマスタ鍵で暗号化したファイルを保存する必要があることから、ファイルのデータ量が多量になり、また暗号化に要する時間が長くなる問題点、マスタ鍵と暗号化データの管理が困難になる問題点、違うマスタ鍵での誤復号によりデータが破壊される可能性がある問題点など、種々の問題点があった。

【0010】

【課題を解決するための手段】本発明の情報処理システムはこのような課題に着目してなされたものであり、その目的とするところは、たとえ装置が盗難されたり分解されたりしても、内部に記憶された機密情報を保護する

ことができる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することにある。

【0011】また、本発明の他の目的は、複数のユーザで共有するデータを、効率的かつ安全に暗号化した形で保存できる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することにある。

【0012】上記の目的を達成するために、第1の発明に係る情報処理システムは、第1の情報処理装置と、この第1の情報処理装置とは別体で構成されており、かつ前記第1の情報処理装置と信号の受渡しが可能な第2の情報処理装置とを具備する情報処理システムであって、前記第1の情報処理装置は、第1の鍵を生成するための第1鍵生成手段と、この第1鍵生成手段によって生成された前記第1の鍵を用いてデータを暗号化して第1暗号情報を生成するための第1暗号化手段とを備え、前記第2の情報処理装置は、第2の鍵を記憶するための第2鍵記憶手段と、この第2鍵記憶手段に記憶された前記第2の鍵を用いて前記第1の鍵を暗号化して第2暗号情報を生成するための第2暗号化手段とを備え、前記第1の情報処理装置は、前記第1暗号化手段によって生成された前記第1暗号情報と、前記第2暗号化手段によって生成された前記第2暗号情報とを関連付けて記憶するための関連付け記憶手段をさらに具備する。

【0013】また、第2の発明は、第1の発明において、前記第1の暗号化手段は、前記第1暗号化情報を生成した後に、前記データを削除する手段を有する。また、第3の発明は、第1の発明において、前記第2鍵記憶手段は複数の第2の鍵を記憶しており、前記第1の情報処理装置は、前記第2の情報処理装置に対して、前記複数の第2の鍵の中から、前記第1の鍵を暗号化するのに用いるべき第2の鍵を指示するための指示手段を有する。

【0014】また、第4の発明に係る情報処理システムは、第1の情報処理装置と、この第1の情報処理装置とは別体で構成されており、かつ前記第1の情報処理装置と信号の受渡しが可能な第2の情報処理装置とを具備する情報処理システムであって、前記第1の情報処理装置は、第1の鍵によりデータを暗号化した第1暗号情報と、第2の鍵により第1の鍵を暗号化した第2暗号情報とを関連付けて記憶するための関連付け記憶手段を備え、前記第2の情報処理装置は、第2の鍵を記憶するための第2鍵記憶手段と、この第2鍵記憶手段に記憶された前記第2の鍵により、前記関連付け記憶手段から読み出された前記第2暗号情報を復号して前記第1の鍵を取出すための第1復号手段とを備え、前記第1の情報処理装置は、前記第1復号手段によって取り出された前記第1の鍵により、前記関連付け記憶手段に記憶された前記第1暗号情報を復号して前記データを得るための第2復

号手段をさらに具備する。

【0015】また、第5の発明に係る情報処理装置は、第1の鍵を生成するための第1鍵生成手段と、この第1鍵生成手段によって生成された前記第1の鍵によりデータを暗号化するための暗号化手段と、前記第1鍵生成手段によって生成された前記第1の鍵を外部情報処理装置へ出力し、該外部情報処理装置内で当該装置内に記憶されている第2の鍵により暗号化された前記第1の鍵を入力するための入力手段と、この入力手段を介して入力される前記暗号化された第1の鍵と、前記暗号化手段によって暗号化された前記データとを関連付けて記憶するための記憶手段とを具備する。

【0016】また、第6の発明は、第5の発明において、前記暗号化手段は、前記データを暗号化した後に、当該データを削除する手段を有する。また、第7の発明は、第5の発明において、前記外部情報処理装置に対して、複数の第2の鍵の中から、前記第1鍵を暗号化するのに用いるべき第2の鍵を指示する指示手段をさらに具備する。

【0017】また、第8の発明に係る情報処理装置は、第1の鍵によりデータを暗号化した第1暗号情報と、第2の鍵により前記第1の鍵を暗号化した第2暗号情報とを記憶するための記憶手段と、この記憶手段に記憶されている前記第2の暗号情報を外部情報処理装置へ出力し、該外部情報処理装置内で当該外部情報処理装置内に記憶されている第2の鍵により前記第2暗号情報を復号して得られる復号された第1の鍵を入力するための入力手段と、この入力手段を介して入力された前記復号された第1の鍵により前記第1暗号情報を復号して前記データを得るための復号化手段とを具備する。

【0018】また、第9の発明に係る情報処理装置は、第2の鍵を記憶するための記憶手段と、第1の鍵を生成し、この第1の鍵によりデータを暗号化する外部情報処理装置から、前記第1の鍵を入力するための入力手段と、前記記憶手段に記憶されている前記第2の鍵によって、前記入力手段を介して入力される前記第1の鍵を暗号化するための暗号化手段と、前記外部情報処理装置において、この暗号化手段によって暗号化された第1の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第1の鍵を前記外部情報処理装置へ出力するための出力手段とを具備する。

【0019】また、第10の発明は、第9の発明において、前記記憶手段は複数の第2の鍵を記憶しており、前記暗号化手段は、この複数の第2の鍵の中から、前記外部情報処理装置によって指示された第2の鍵によって前記第1の鍵を暗号化する手段を有する。

【0020】また、第11の発明に係る情報処理装置は、第2の鍵を記憶するための記憶手段と、第1の鍵によりデータを暗号化して得られる第1暗号情報と、前記記憶手段に記憶された前記第2の鍵により、前記第1の

鍵を暗号化して得られる第2暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から、前記第2暗号情報を入力するための入力手段と、この入力手段を介して入力された前記第2暗号情報を前記第2の鍵により復号して前記第1の鍵を取出すための復号手段と、前記外部情報処理装置において、前記復号手段により取り出された前記第1の鍵により前記第1暗号情報を復号して前記データを得るために、前記取り出された第1の鍵を前記外部情報処理装置へ出力するための出力手段とを具備する。

【0021】また、第12の発明に係る情報処理方法は、第1の情報処理装置内で第1の鍵を生成する第1鍵生成工程と、生成された第1の鍵を用いてデータを暗号化して第1暗号情報を生成する第1暗号情報生成工程と、生成された第1の鍵を、前記第1の情報処理装置とは別体で構成され、第2の鍵を記憶している第2の情報処理装置へ出力する出力工程と、前記第2の情報処理装置内で前記第2の鍵を用いて前記第1の鍵を暗号化して第2暗号情報を生成する第2暗号情報生成工程と、生成された第2暗号情報を前記第1の情報処理装置へ出力する出力工程と、前記第1情報処理装置内で前記第1暗号情報と前記第2暗号情報とを関連付けて記憶する記憶工程とを具備する。

【0022】また、第13の発明に係る情報処理方法は、第1の鍵によりデータを暗号化して得られた第1暗号情報と、第2の鍵により前記第1の鍵を暗号化して得られた第2暗号情報とが関連付けて記憶されている第1の情報処理装置内から、前記第2暗号情報を、当該第1の情報処理装置とは別体で構成された第2の情報処理装置へ出力する出力工程と、前記第2の情報処理装置内に予め記憶されている前記第2の鍵により、前記第2暗号情報を復号して前記第1の鍵を取り出す第1鍵取り出し工程と、取り出された第1の鍵を前記第1の情報処理装置へ出力する出力工程と、前記第1の情報処理装置において、当該第1の鍵により前記第1暗号情報を復号して前記データを得るデータ取得工程とを具備する。

【0023】また、第14の発明に係る情報処理方法は、第1の鍵を生成する第1鍵生成工程と、生成された第1の鍵によりデータを暗号化する暗号化工程と、生成された第1の鍵を外部情報処理装置へ出力する出力工程と、当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第2の鍵により暗号化された第1の鍵を入力する入力工程と、入力された前記暗号化された第1の鍵と、前記第1の鍵により暗号化されたデータとを関連付けて記憶する記憶工程とを具備する。

【0024】また、第15の発明に係る情報処理方法は、第1の鍵によりデータを暗号化して記憶された第1暗号情報と、第2の鍵により第1の鍵を暗号化して記憶された第2暗号情報のうち、前記第2の暗号情報を外部情報処理装置へ出力する出力工程と、該外部情報処理装

置内で当該外部情報処理装置内に記憶されている前記第2の鍵により前記第2暗号情報を復号して得られた前記第1の鍵を入力する入力工程と、入力された前記第1の鍵により前記第1暗号情報を復号して前記データを取り出す取り出し工程とを具備する。

【0025】また、第16の発明に係る情報処理方法は、生成された第1の鍵によりデータを暗号化する外部情報処理装置から前記第1の鍵を入力する入力工程と、予め記憶されている第2の鍵により入力された前記第1の鍵を暗号化する暗号化工程と、前記外部情報処理装置において、この暗号化された第1の鍵と、前記暗号化されたデータとを関連付けて記憶するために、前記暗号化された第1の鍵を前記外部情報処理装置へ出力する出力工程とを具備する。

【0026】また、第17の発明に係る情報処理方法は、第1の鍵によりデータを暗号化して得られた第1暗号情報と、第2の鍵により第1の鍵を暗号化して得られた第2暗号情報とを記憶するための記憶手段を備えた外部情報処理装置から前記第2暗号情報を入力する入力工程と、予め記憶している第2の鍵により前記第2暗号情報を復号して前記第1の鍵を取出す取り出し工程と、前記外部情報処理装置において、取り出された前記第1の鍵により前記第1暗号情報を復号して前記データを得るために、復号により取り出された前記第1の鍵を前記外部情報処理装置へ出力する出力工程とを具備する。

【0027】また、第18の発明にプログラム記憶装置は、暗号化処理を実行する方法ステップを遂行するために、マシンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、前記方法ステップは、第1の鍵を生成する第1鍵生成ステップと、生成された第1の鍵によりデータを暗号化する暗号化ステップと、生成された第1の鍵を外部情報処理装置へ出力する出力ステップと、当該外部情報処理装置内で当該外部情報処理装置内に記憶されている第2の鍵により暗号化された第1の鍵を入力する入力ステップと、入力された前記暗号化された第1の鍵と、前記第1の鍵により暗号化されたデータとを関連付けて記憶する記憶ステップとを具備する。

【0028】また、第19の発明に係るプログラム記憶装置は、暗号化処理を実行する方法ステップを遂行するために、マシンによってリーダブルなプログラムを記憶したプログラム記憶装置であって、前記方法ステップは、第1の鍵によりデータを暗号化して記憶された第1暗号情報と、第2の鍵により第1の鍵を暗号化して記憶された第2暗号情報のうち、前記第2の暗号情報を外部情報処理装置へ出力する出力ステップと、該外部情報処理装置内で当該外部情報処理装置内に記憶されている前記第2の鍵により前記第2暗号情報を復号して得られた前記第1の鍵を入力する入力ステップと、入力された前記第1の鍵により前記第1暗号情報を復号して前記デー

タを取り出す取り出しステップとを具備する。

【0029】また、第20の発明に係る鍵の判定方法は、送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第2の鍵の中から受信側で有している特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定方法において、前記第1の鍵を前記複数の第2の鍵でそれぞれ暗号化あるいは復号化して得られた第1データを入力する入力工程と、前記第1データの中で前記特定の第2の鍵で暗号化あるいは復号化された特定の第1データと所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力工程と、入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出工程と、抽出された前記特定の第2の鍵を出力する出力工程とを具備する。

【0030】また、第21の発明に係る鍵の判定方法は、送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵の中の特定の第2の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第2の鍵の中から前記特定の第2の鍵を抽出するための鍵の判定方法において、前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する入力工程と、前記第1データと所定の処理を行なうことにより、前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力工程と、入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出工程と、抽出された前記特定の第2の鍵を出力する出力工程とを具備する。

【0031】また、第22の発明に係る鍵の判定方法は、送信側で、データを暗号化するのに用いた第1の鍵を送信側及び受信側が共に有している複数の第2の鍵の中から、特定の第2の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定方法であって、前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する入力工程と、前記第1データの中と所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力工程と、入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出工程と、抽出された前記特定の第2の鍵を出力する出力工程とを具備する。

【0032】また、第23の発明に係る鍵の判定装置は、送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第2の鍵の中から受信側で

有している特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定装置であって、前記第1の鍵を前記複数の第2の鍵でそれぞれ暗号化あるいは復号化して得られた第1データを入力する第1入力手段と、この第1入力手段によって入力された前記第1データの中で、前記特定の第2の鍵で暗号化あるいは復号化された特定の第1データと所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する第2入力手段と、この第1入力手段によって入力された前記第1データと、前記第2入力手段によって入力された前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出手段と、この抽出手段によって抽出された前記特定の第2の鍵を出力する出力手段とを具備する。

【0033】また、第24の発明は、第23の発明において、前記第2のデータを前記第1の鍵と前記第2の鍵とに基づいて生成する第1生成手段と、前記第2のデータを前記第1の鍵のみに基づいて生成する第2生成手段と、前記第2データを前記第2の鍵のみに基づいて生成する第3生成手段と、前記第2データを前記第1の鍵と前記第2の鍵のいずれをも使用しないで生成する第4の生成手段をさらに具備する。

【0034】また、第25の発明は、第24の発明において、前記第1生成手段は、前記第2の鍵を前記第1の鍵で暗号化して得られるデータと、前記第2の鍵を前記第1の鍵で復号して得られるデータと、前記第1の鍵を前記第2の鍵で2回暗号化して得られるデータと、前記第1の鍵を前記第2の鍵で復号して得られるデータのいずれかを選択的に生成する。

【0035】また、第26の発明は、第24の発明において、前記第2生成手段は、前記第1の鍵をこの第1の鍵で暗号化して得られるデータと、前記第1の鍵をこの第1の鍵で復号して得られるデータと、所定の共有データを前記第1の鍵で暗号化して得られるデータと、所定の共有データを前記第1の鍵で復号して得られるデータと、前記第1の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【0036】また、第27の発明は、第24の発明において、前記第3生成手段は、前記第2の鍵をこの第2の鍵で暗号化して得られるデータと、前記第2の鍵を前記第2の鍵で復号して得られるデータと、前記第2の鍵と暗号化ごとに変更される共有データとを加算したものを前記第2の鍵で暗号化して得られるデータと、前記第2の鍵と暗号化ごとに変更される共有データとを加算したものを前記第2の鍵で復号して得られるデータと、暗号化ごとに変更される共有データを前記第2の鍵で暗号化して得られるデータと、暗号化ごとに変更される共有データを前記第2の鍵で復号して得られるデータと、前記第2の鍵を特定の関数で暗号化して得られるデータのい

ずれかを選択的に生成する。

【0037】また、第28の発明は、第24の発明において、前記第4生成手段は、前記第1の鍵と前記第2の鍵とを並置したデータを特定の関数で暗号化して得られるデータを生成する。

【0038】また、第29の発明に係る鍵の判定装置は、送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵の中の特定の第2の鍵で暗号化あるいは復号して送信し、受信側で、前記複数の第2の鍵の中から前記特定の第2の鍵を抽出するための鍵の判定装置であって、前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する第1入力手段と、この第1入力手段によって入力された前記第1データと所定の処理を行なうことにより、前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する第2入力手段と、この第2入力手段によって入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出手段と、この抽出手段によって抽出された前記特定の第2の鍵を出力する出力手段とを具備する。

【0039】また、第30の発明は、第29の発明において、前記第2データを前記第1の鍵と前記第2の鍵とに基づいて生成する第1生成手段と、前記第2のデータを前記第1の鍵のみに基づいて生成する第2生成手段と、前記第2データを前記第2の鍵のみに基づいて生成する第3生成手段と、前記第2データを前記第1の鍵と前記第2の鍵のいずれをも使用しないで生成する第4の生成手段をさらに具備する。

【0040】また、第31の発明は、第30の発明において、前記第1生成手段は、前記第2の鍵を前記第1の鍵で暗号化した得られるデータと、前記第2の鍵を前記第1の鍵で復号して得られるデータと、前記第1の鍵を前記第2の鍵で2回暗号化して得られるデータと、前記第1の鍵を前記第2の鍵で復号して得られるデータのいずれかを選択的に生成する。

【0041】また、第32の発明は、第30の発明において、前記第2生成手段は、前記第1の鍵をこの第1の鍵で暗号化して得られるデータと、前記第1の鍵をこの第1の鍵で復号して得られるデータと、所定の共有データを前記第1の鍵で暗号化して得られるデータと、所定の共有データを前記第1の鍵で復号して得られるデータと、前記第1の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【0042】また、第33の発明は、第30の発明において、前記第3判定手段は、前記第2の鍵をこの第2の鍵で暗号化して得られるデータと、前記第2の鍵を前記第2の鍵で復号して得られるデータと、前記第2の鍵と暗号化ごとに変更される共有データとを加算したものを前記第2の鍵で暗号化して得られるデータと、前記第2

の鍵と暗号化ごとに変更される共有データとを加算したものを前記第2の鍵で復号して得られるデータと、暗号化ごとに変更される共有データを前記第2の鍵で暗号化して得られるデータと、暗号化ごとに変更される共有データを前記第2の鍵で復号して得られるデータと、前記第2の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【0043】また、第34の発明は、第30の発明において、前記第4生成手段は、前記第1の鍵と前記第2の鍵とを並置したデータを特定の関数で暗号化して得られるデータを生成する。

【0044】また、第35の発明に係る鍵の判定装置は、送信側で、データを暗号化するのに用いた第1の鍵を送信側及び受信側が共に有している複数の第2の鍵の中から、特定の第2の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出するための鍵の判定装置であって、前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する第1入力手段と、この第1入力手段によって入力された前記第1データの中と所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する第2入力手段と、前記第1入力手段によって入力された前記第1データと、前記第2入力手段によって入力された前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出手段と、この抽出手段によって抽出された前記特定の第2の鍵を出力する出力手段とを具備する。

【0045】また、第36の発明は、第35の発明において、前記第2データを前記第1の鍵と前記第2の鍵とに基づいて生成する第1生成手段と、前記第2のデータを前記第1の鍵のみに基づいて生成する第2生成手段と、前記第2データを前記第2の鍵のみに基づいて生成する第3生成手段と、前記第2データを前記第1の鍵と前記第2の鍵のいずれをも使用しないで生成する第4の生成手段をさらに具備する。

【0046】また、第37の発明は、第36の発明において、前記第1生成手段は、前記第2の鍵を前記第1の鍵で暗号化した得られるデータと、前記第2の鍵を前記第1の鍵で復号して得られるデータと、前記第1の鍵を前記第2の鍵で2回暗号化して得られるデータと、前記第1の鍵を前記第2の鍵で復号して得られるデータのいずれかを選択的に生成する。

【0047】また、第38の発明は、第36の発明において、前記第2生成手段は、前記第1の鍵をこの第1の鍵で暗号化して得られるデータと、前記第1の鍵をこの第1の鍵で復号して得られるデータと、所定の共有データを前記第1の鍵で暗号化して得られるデータと、所定の共有データを前記第1の鍵で復号して得られるデータ

と、前記第1の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【0048】また、第39の発明は、第36の発明において、前記第3生成手段は、前記第2の鍵をこの第2の鍵で暗号化して得られるデータと、前記第2の鍵を前記第2の鍵で復号して得られるデータと、前記第2の鍵と暗号化ごとに変更される共有データとを加算したものを前記第2の鍵で暗号化して得られるデータと、前記第2の鍵と暗号化ごとに変更される共有データとを加算したものを前記第2の鍵で復号して得られるデータと、暗号化ごとに変更される共有データを前記第2の鍵で暗号化して得られるデータと、暗号化ごとに変更される共有データを前記第2の鍵で復号して得られるデータと、前記第2の鍵を特定の関数で暗号化して得られるデータのいずれかを選択的に生成する。

【0049】また、第40の発明は、第36の発明において、前記第4生成手段は、前記第1の鍵と前記第2の鍵とを並置したデータを特定の関数で暗号化して得られるデータを生成する。

【0050】また、第41の発明に係るプログラム記憶装置は、送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵でそれぞれ暗号化あるいは復号して送信し、受信側で、前記複数の第2の鍵の中から受信側で有している特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、前記判定ステップは、前記第1の鍵を前記複数の第2の鍵でそれぞれ暗号化あるいは復号化して得られた第1データを入力する入力ステップと、前記第1データの中で前記特定の第2の鍵で暗号化あるいは復号化された特定の第1データと所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力ステップと、入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出ステップと、抽出された前記特定の第2の鍵を出力する出力ステップとを具備する。

【0051】また、第42の発明に係るプログラム記憶装置は、送信側で、データを暗号化するのに用いた第1の鍵を複数の第2の鍵の中の特定の第2の鍵で暗号化あるいは復号化して送信し、受信側で、前記複数の第2の鍵の中から前記特定の第2の鍵を抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、前記判定ステップは、前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する入力ステップと、前記第1データと所定の処理を行なうことにより、前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力ステ

ップと、入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出ステップと、抽出された前記特定の第2の鍵を出力する出力ステップとを具備する。

【0052】また、第43の発明に係るプログラム記憶装置は、送信側で、データを暗号化するのに用いた第1の鍵を送信側及び受信側が共に有している複数の第2の鍵の中から、特定の第2の鍵で暗号化あるいは復号して送信し、受信側で、前記特定の第2の鍵に該当する第2の鍵を前記複数の第2の鍵の中から抽出して鍵の判定を行なう判定ステップを遂行するために、マシンリーダブルなプログラムを記憶したプログラム記憶装置であって、前記判定ステップは、前記第1の鍵を前記特定の第2の鍵で暗号化あるいは復号して得られた第1データを入力する入力ステップと、前記第1データの中と所定の処理を行なうことにより前記特定の第2の鍵が得られるような処理によって処理された第2データを入力する入力ステップと、入力された前記第1データと前記第2データとに基づいて、前記所定の処理を行なうことにより前記特定の第2の鍵を抽出する抽出ステップと、抽出された前記特定の第2の鍵を出力する出力ステップとを具備する。

【0053】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態を詳細に説明する。図1は、本発明の第1の実施の形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、暗号化を行なう場合の装置構成を示す図である。

【0054】本発明の情報処理システムは、情報処理装置としての携帯型パーソナルコンピュータ（以下携帯型PCと呼ぶ）6と、この携帯型PC6に着脱可能に装着された外部記憶装置としてのICカード5とからなる。

【0055】図1において、携帯型PC6内部に設けられた第1鍵生成手段としての乱数生成器3によって生成された一時鍵（第1の鍵）は暗号化装置4（第1暗号化手段）に転送される。また、携帯型PC6内部の例えばハードディスク装置等から成る記憶装置12内に一時的に記憶されている機密情報を含むファイル1も、暗号化装置4に転送される。

【0056】この暗号化装置4において機密情報を含むファイル1に対する暗号化が行われて暗号化ファイル2の第1の暗号化データとしてのボディ部8となる。一方、乱数発生器3によって生成された一時鍵は同時に外部インターフェース（以下外部I/Fと呼ぶ）7を介してICカード5内部の第2の暗号化手段としての暗号化装置10にも転送される。暗号化装置10はマスター鍵記憶部（第2鍵記憶手段）9に記憶されているマスター鍵（第2の鍵）を用いて、転送された一時鍵を暗号化し、暗号化された一時鍵は外部I/F7を介して携帯型

PC6内部の記憶装置（関連付け記憶手段）12に転送されて暗号化ファイル2の第2の暗号化データとしてのヘッダー部11となる。

【0057】また、ICカード5内に乱数発生器3を設けて、ICカード3の内部で一時鍵を生成することも可能である。このようにすれば携帯型PC6とのデータ転送回数を減らすことができる。

【0058】このようにしてファイル1に対する暗号化が行われ、ヘッダー11とボディ部8とを合成することにより得られた暗号化ファイル2は記憶装置12に記憶されると同時に、元のファイル1を消去する。

【0059】図2は、暗号化を行った後の携帯型情報処理システムの構成の変更を示す図である。つまり、ファイル1を暗号化して暗号化ファイル2として記憶装置12に記憶する一方で、元の機密情報を含むファイル1は記憶装置12内からは削除される。またマスター鍵を記憶しているICカード5を携帯型PC6から取り外し、携帯型PC6とICカード5とを別々に保管する。

【0060】すなわち、暗号化ファイル2として記憶されるのは、元のファイル1を暗号化した情報（ボディ部8）と暗号化の時に使用した一時鍵をマスター鍵で暗号化した情報（ヘッダー部11）であり、いずれも暗号化された情報である。この暗号ファイル2のみを記憶した携帯型PC6が仮に盗難にあったとしても、マスター鍵を記憶したICカード5を携帯型PC6と別に保管しておくことにより、マスター鍵と暗号化情報が同時に盗難にあうことを防止でき、機密情報の漏洩は防止される。

【0061】なお、携帯型PC6内部の暗号化装置4で使用されるアルゴリズムと、ICカード5内部の暗号化装置10で使用されるアルゴリズムは同一のものであってもよいし、異なるアルゴリズムであってもよい。

【0062】また、暗号化のための一時鍵は乱数発生装置により発生されたものなので例えば、ファイル毎に異なるものであり、より安全性が高まっている。図3は本発明の第1の実施の形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、復号化を行なう場合の装置構成を示す図である。

【0063】この図3は、基本的に図1に示したシステム構成図に対して、暗号化の機能と復号化の機能を入れ替えた構成に対応し、実際の情報処理システムでは、これら暗号化の機能と復号化の機能の双方を備えたものが用いられる。ここでは、図1の暗号化の機能と図3に示す復号化の機能が同一の携帯型情報処理システム内で処理されることを想定し、同一構成、同一要素には同一記号を付して説明する。

【0064】図3における情報処理システムは、情報処理装置としての携帯型PC6と、この携帯型PC6に着脱可能に装着された外部記憶装置としてのICカード5とからなる。

【0065】図3において、携帯型PC6内部の暗号化

ファイル2はヘッダー部11とボディ部8とに分解され、ヘッダー部11は外部I/F7を介してICカード5内部の第1の復号手段としての復号装置20に転送される。復号装置20はマスター鍵記憶部9に記憶されているマスター鍵を用いて復号を行って暗号化時に使用された元の一時鍵を抽出し、抽出された一時鍵を外部I/F7を介して携帯型PC6内部の第2復号手段としての復号装置14に転送する。復号装置14はこの一時鍵を用いて分解されたボディ部8の復号を行って元のファイル1を得る。

【0066】以上、上記した第1の実施の形態によれば、暗号化ファイルは、携帯型PCに対して着脱可能に装着されたICカードに格納されたマスター鍵により暗号化した上で内部のハードディスクに保存されているので、ICカードを装着しない限りファイルの復号はできない。したがってICカードをPCとは別に携帯するようにすれば、たとえ携帯型PCが盗難されても機密情報は安全に保護される。

【0067】また、ファイル自体の暗号化は一時鍵を用いて携帯型PCの内部を行い、外部から装着されるICカードでは一時鍵のみをマスター鍵によって暗号化しているので、暗号化の効率が向上するとともに、携帯型PCの内部にはマスター鍵が読み込まれることがなく、かつ2重に暗号化を行っていることになるので、機密情報の安全性がより向上する。

【0068】また、計算能力のあるICカード内にマスター鍵を格納した場合でも、マスター鍵自体は携帯型PC内に読み込まれて記憶されることはないので、例えば、トロイの木馬などのようなプログラムが携帯型PC内に組み込まれてもマスター鍵を不正な第三者に知られることはない。

【0069】また、計算能力の異なるICカードを適宜選択的に用いるようにすれば、暗号化、復号化時の処理を高速化することが可能である。これより、処理速度を重視しない場合は処理能力の劣るICカードを用いてもよい。

【0070】また、ファイル毎に鍵を変更しているので安全性がより高い。さらに、仮にマスター鍵が知られてしまってもファイルを再び暗号化しなおさなければならない場合であっても、ヘッダー部のみを暗号化しなおすだけでよいので、短時間に暗号化を行うことができるという効果を奏する。

【0071】また、DES暗号においては、十分な数のファイルと暗号化ファイルとの対を収集することによって暗号化に用いられた鍵を導き出されることが知られているが、上記した実施形態によれば、ファイルを暗号化するたび鍵に変更している上に、マスター鍵による暗号化部分に対応する平文ファイルが復号時に携帯型PC内に格納されることはないので、ファイルの収集そのものが不可能であり、仮にファイルの収集ができたとして

も、十分な数のファイルが収集されるまで暗号化処理を繰り返すことは実質的に不可能である。すなわち、マスター鍵によりファイルを直接暗号化する方法では、たとえ数回の暗号化であっても、暗号化するファイルが十分に長ければ暗号化に用いられた鍵を導き出すことができる場合があるが、本実施形態ではマスター鍵自体はファイルを直接暗号化するためには用いられないので、十分に長いファイルを暗号化しても、鍵を導き出すのに十分なファイルを収集することはできない。

10 【0072】なお、上記した実施形態ではマスター鍵で暗号化した一時鍵を記憶するヘッダー部が1つの場合について説明したが、ヘッダー部は複数であってもよい。例えば、1台のPCを複数人で構成されるグループ内で使用して情報を共有したい場合は、各人が個々に使用する暗号化鍵と、そのグループ内で共通に使用できる暗号化鍵とが必要になるので、ヘッダー部は複数用意することになる。また、あらかじめ複数のヘッダー部を設けて複数の人が内部のファイルにアクセスできるようにしておくことにより、何らかの理由でアクセスできなくなった人の代わりに他の人がアクセスして情報を得ることができる。

20 【0073】また、上記した実施形態では携帯型PCに着脱可能なICカードを用いて情報処理装置と外部記憶装置との間で信号の受け渡しを行っているが、機械的に着脱可能に構成されていなくとも、例えば赤外線、無線、光（レーザ光等）通信などの方法により、情報処理装置と外部記憶装置との間で信号を受け渡すように構成してもよい。

30 【0074】図4は、本発明の第2実施形態として、図1乃至図3に示した情報処理システムに適用することが可能な、鍵の判定方法を実現するための鍵判定システムの構成図である。特に、図4は復号時に用いられるマスター鍵を判定しながら、一時鍵を取り出す場合の装置構成を示す図である。ここでは暗号化時に、例えば図1のマスター鍵記憶部9に記憶されたマスター鍵を用いて暗号化された一時鍵をさらにマスター鍵で暗号化して得られた一時鍵（マスター鍵によって2回暗号化した一時鍵：第3の暗号化データ）が暗号化ファイルのヘッダー部11にあらかじめ記憶されているものとする。

40 【0075】そして、復号時には、図4に示すように第3の暗号化データとしての2回暗号化した一時鍵23と、第2の暗号化データとしての1回暗号化した一時鍵24とがICカード5に供給される。復号装置20aは、マスター鍵記憶部9に記憶されたマスター鍵（特定のマスター鍵）を用いて2回暗号化した一時鍵23を復号して復号された一時鍵を出力する。比較部27はこの復号された一時鍵と、一回暗号化した一時鍵24とを比較して比較結果を一致判定部33に供給する。一致判定部33はこの比較結果に基づいて、復号された一時鍵と
50 1回暗号化した一時鍵とが一致するか否かを判定する。

【0076】そして、一致すると判定された場合は一致信号28によってスイッチ34を閉じ、復号装置20aからの復号された一時鍵を復号装置20bにおいてマスター鍵記憶部9に記憶されたマスター鍵を用いてさらに復号して元の一時鍵31を得る。なお、図3のシステムに適用される場合には、ここで得られた元の一時鍵31は、携帯型PC6へ転送されて暗号ファイル2の復号に使用される。なお、復号装置20aと20bとは、機能ブロック上、2つの復号装置として示したが、実際には1つの復号化装置で良い。

【0077】また、一致判定部33で復号された一時鍵と1回暗号化した一時鍵24が一致しないと判定された場合は、不一致信号29が出力されてNGの状態32が得られる。

【0078】以上、上記した第2の実施の形態によれば、2回暗号化した一時鍵をマスター鍵によって復号した一時鍵と、1回暗号化した一時鍵とを比較することによって一致した場合は、復号に使用したマスター鍵が暗号化時に用いられたマスター鍵と同じ鍵であると判定することができ、一致しない場合は暗号化時に使用されたマスター鍵とは異なるマスター鍵によって一時鍵が復号されたと判定することができる。

【0079】したがって、一致しない場合は当該マスター鍵を使用不可にすることにより、機密ファイルの漏洩を防止することができるとともに、誤ってファイルを破壊してしまうことを防止することができる。さらに、一台の携帯型PCを複数人で使用する場合には、他人が暗号化したファイルを誤って復号してしまったときは一時鍵が失われてしまうので、もう一度暗号化しても元のファイルを復元することができないが、上記したように1回暗号化した一時鍵と、2回暗号化した一時鍵を復号した鍵とが一致しない場合は復号が行われないので、誤った一時鍵による復号を防止することができる。

【0080】なお、上記した図4の装置を構成を簡略化すると図5に示すような構成となる。図5において、 S_k は一時鍵、 M_k はマスター鍵を表し、一時鍵 S_k をマスター鍵 M_k によって1回暗号化して得られるデータ（図4の24）を $M_k(S_k)$ で表す。また、Dは復号を表している。 $M_k^2(S_k)$ はマスター鍵によって2回暗号化して得られるデータ（図4の23）を表している。51、52は復号装置であり、図4の復号装置20a、20bにそれぞれ対応する。また、53は比較判定部であり、図4の比較部27、一致判定部33に対応する。

【0081】図6は図5に示す装置構成の変形例を示す図であり、2つの復号装置54、56と、比較判定部55と、スイッチ50とから構成される。このような構成によれば、図5に示す構成と比較して復号装置54、56での復号処理が同時に行われるので、処理が高速であるという利点がある。

【0082】図7は図5に示す装置構成の他の変形例を示す図であり、暗号化装置57と、復号装置58と、比較判定部59とから構成される。このような構成によれば、図6では2つの復号装置が必要になるのに対して、暗号化時の暗号化装置10を暗号化装置57として使用することができ、かつ、暗号化装置57での暗号化処理と復号装置58での復号処理が同時に行われるので処理が高速であるという利点がある。

【0083】上記した第1、第2実施形態によれば、本発明によれば、たとえ装置が盗難されたり分解されたりしても、内部に記憶された機密情報を保護することができるようになる。また、誤ったマスター鍵による復号に起因するファイルの破壊や機密情報の漏洩を防止することができる。

【0084】図8は、本発明の第3実施形態に係る情報処理システム（暗号側）の構成を示す図である。本実施形態に係る情報処理システムは、概略的には、暗号側となる情報処理装置において、所定の一時鍵を生成し、これを用いて暗号化対象となるデータを暗号化するとともに、この一時鍵の暗号化を、マスター鍵を記憶している処理機能付き外部記憶装置に依頼し、処理機能付き外部記憶装置において、受け取った一時鍵に対し、自装置内に記憶されている所定のマスター鍵を用いた所定の暗号化を施して、情報処理装置に暗号化鍵を戻すものである。

【0085】また、外部記憶装置の内部で一時鍵を発生させることも可能である。このようにすれば情報処理装置との間のデータ転送回数を減らすことができる。同様に、本実施形態に係る情報処理システムは、概略的には、復号側となる情報処理装置において、暗号化データに含まれる一時鍵とマスター鍵をもとにした暗号化鍵の復号化を、マスター鍵を記憶している処理機能付き外部記憶装置に依頼し、処理機能付き外部記憶装置において、受け取った暗号化鍵の情報と自装置内に記憶されている所定のマスター鍵をもとに、所定の復号化を行って、もとの一時鍵を取り出し、これを情報処理装置に戻し、情報処理装置において、渡された一時鍵を用いて、暗号化されたデータを復号するものである。

【0086】各情報処理装置は、単一ユーザであっても、複数ユーザで共用するものであっても良い。ただし、後述するマスター鍵を保管した処理機能付き外部記憶装置は、ユーザ毎に容易するのが望ましい。

【0087】本実施形態では、あるデータaを鍵Kを用いて暗号化する操作を $E_K(a)$ と表現し、あるデータaを鍵Kを用いて復号化する操作を $D_K(a)$ と表現する。この表現を用いることにより、例えば、あるデータaを鍵K1を用いて暗号化し鍵K2を用いて復号する操作は、 $D_{K2}(E_{K1}(a))$ で表される。

【0088】なお、本実施形態では、暗号化対象となるデータの暗号方式と、このデータの暗号化や復号化に使用する一時鍵の暗号方式には、DESあるいはFEAL

のである。

【0118】次に、これら $E_{Mki}(S_k)$ と $E_{Sk}(S_k)$ を、情報処理装置101に送信する(ステップS18)。情報処理装置101側では、これら $E_{Mki}(S_k)$ と $E_{Sk}(S_k)$ を受信すると(ステップS19)、暗号化データ生成部6により、 $E_{Mki}(S_k)$ と $E_{Sk}(S_k)$ をヘッダ部に含み、 $E_{Sk}(\text{Data})$ をデータ部とするファイルやパケットなどの暗号化データを作成する(ステップS20)。

【0119】以上のようにして生成された暗号化データは、所定の記憶装置に保存され、あるいはネットワークなどを介して所望の宛先装置(復号側となる情報処理装置)に転送される。

【0120】ここで、暗号化されたデータ $E_{Sk}(\text{Data})$ を解読するためには、 $E_{Mki}(S_k)$ を解読して一時鍵を取り出す必要がある。復号側で該当するマスタ鍵を所有する場合にのみデータ Data を取り出すことができる。例えば、 M_{k1} 、 M_{k2} 、 M_{k3} をそれぞれ用いて一時鍵 S_k を暗号化した場合、暗号化データのヘッダ部には、 $E_{Mk1}(S_k)$ 、 $E_{Mk2}(S_k)$ 、 $E_{Mk3}(S_k)$ が含まれるので、 M_{k1} 、 M_{k2} 、 M_{k3} のいずれかのマスタ鍵を持つものが、平文のデータ Data を得ることができる。なお、言うまでもなく、ヘッダ部の情報から一時鍵やマスタ鍵を解読するのはきわめて困難である。

【0121】また、復号側では、ヘッダ部に含まれる一時鍵自身で暗号化された一時鍵 $E_{Sk}(S_k)$ をもとにして、復号した一時鍵の検証を行うことができる。さらに、1つの暗号化データを解読可能とするマスタ鍵の数にかかわらず、上記検証のために付加する情報は、一時鍵自身で暗号化された一時鍵のただ1つのみで良く、マスタ鍵の個数に相当する回数(マスタ鍵の暗号化と1回だけの一時鍵自身の暗号化を行うことにより、全てのマスタ鍵に対する検証を施すことができるので、同一データに対する複数のマスタ鍵の使用が容易になる。

【0122】例えば、各々のマスタ鍵で一時鍵を1回暗号化したものと2回暗号化したものを組にしてヘッダに格納し、復号化の際、同じマスタ鍵で同じ一時鍵を1回と2回復号化した2種類の一時鍵の一致判定を行うことにより、マスタ鍵の検証を行うこともできる。しかし、この方法によると、ヘッダに格納する暗号化された一時鍵の情報は、マスタ鍵の個数の2倍に相当するサイズになる。これに対して、上記の各々のマスタ鍵による一時鍵の暗号化と一時鍵自身による一時鍵の暗号化では、マスタ鍵の個数+1に相当する情報だけをヘッダに格納することができ、ヘッダサイズを小さく抑えることができる。

【0123】なお、一時鍵は少なくともデータ毎に生成されるので、たとえある暗号化データの一時鍵が解読されたとしても、他の暗号化データをその一時鍵で解読することはできない。

【0124】次に、復号側の情報処理システムについて説明する。図14は、本発明の一実施形態に係る情報処理システムにおいて、復号化を行う側の情報処理装置111と外部記憶装置112の構成を示す図である。

【0125】情報処理装置111は、データの復号化などを行うものである。情報処理装置111には、例えば、パーソナルコンピュータを用いることができる。外部記憶装置112は、マスタ鍵の保管、一時鍵の復号などを行うものである。外部記憶装置112には、例えば、処理機能を有するICカードを用いることができる。

【0126】情報処理装置111と外部記憶装置112とは、それぞれの持つインタフェース部(図示せず)を介して、データの受け渡しを行う。例えば、使用時に外部記憶装置112を情報処理装置111内のソケットに直接接続する方法を用いても良いし、赤外線などにより通信できるようにしても良い。

【0127】なお、外部記憶装置112を使用しないときは、これをユーザが安全な場所に保管しておくのが好ましい。さて、図14に示すように、復号を行う側の情報処理装置111は、暗号化データ保持部116、復号化部114、復号化データ保持部113を備えている。

【0128】暗号化データ保持部116は、復号化対象となる暗号化データを保持するためのものである。復号化の対象である暗号化データは、所定の記憶装置から読出したものでも良いし、有線や無線の通信回線を介して取得したものでも良い。

【0129】ここで、暗号化データ保持部116に保持されている暗号化データのヘッダ部に含まれるマスタ鍵で暗号化された一時鍵と一時鍵自身で暗号化された一時鍵の情報は、インタフェース部を介して外部記憶装置112に渡される。なお、外部記憶装置112にヘッダ部全体を送信するようにしても良い。

【0130】また、上記暗号化データのデータ部に含まれる一時鍵で暗号化されたデータは、復号化部114に渡される。復号化部114では、外部記憶装置112からインタフェース部を介して返された一時鍵を用いて、上記の一時鍵で暗号化されたデータを復号化する。

【0131】復号化データ保持部113は、この復号化により得られた平文のデータを保持するためのものである。なお、復号化により得られたデータは、例えば、CRTや液晶などの表示装置に表示され、あるいは画像や音声の再生装置に出力され、あるいはこの情報処理装置111の内蔵ハードディスク等の記憶装置あるいはフロッピーディスクやCD-ROMなどのリムーバブルな記憶媒体にファイルとして格納され、あるいはLANを介してファイル管理装置に転送され、あるいはパケットやセルの形にして有線や無線の通信回線を介して所望の転送先に送り出される。

【0132】次に、一時鍵の復号化を行う側の外部記憶

装置112について説明する。この外部記憶装置112は、マスタ鍵の情報を保管する機能を持つとともに、このマスタ鍵のデータ自体を自装置の外部に出さずに、情報処理装置111から渡された所定のマスタ鍵で暗号化された一時鍵の情報をもとに復号化処理を全て自装置内で行ってその結果得られた一時鍵（または復号不可を示す制御信号）を情報処理装置111に返す働きを持つものである。

【0133】図14に示すように、一時鍵の復号化を行う側の外部記憶装置112は、マスタ鍵記憶部119、
10 復号化部118を備えている。マスタ鍵記憶部119は、1または複数のマスタ鍵を記憶する。

【0134】このマスタ鍵記憶部119は、自装置外部からの読出しや書き込みなどのアクセスを不可とするのが望ましい。ただし、パスワード・チェックなどの認証に通過すれば、マスタ鍵の情報の追加、削除などの操作が可能となるようにしても良い。

【0135】復号化部118は、インタフェース部を介して情報処理装置111から送信されたマスタ鍵で暗号化された一時鍵および一時鍵自身で暗号化された一時鍵
20 を受け取り、マスタ鍵記憶部119内に記憶されているマスタ鍵を用い復号化を行って、平文の一時鍵を得ることと、鍵の検証とを同時に行う。

【0136】図15は、本発明の第4実施形態に係る鍵の判定を実現するための鍵判定システムの構成を示す図である。1または複数のマスタ鍵でそれぞれ暗号化された一時鍵および一時鍵自身で暗号化された一時鍵が、インタフェース部を介して情報処理装置111から送信されると、復号化部281にて、マスタ鍵記憶部119に格納されているマスタ鍵を用いて、マスタ鍵で暗号化された一時鍵を復号する。この復号化された一時鍵を用いて、復号化部282にて、一時鍵自身で暗号化された一時鍵を復号する。そして、2つの一時鍵が一致するか否かを一致判定部283により判定する。2つの一時鍵が一致しないならば、マスタ鍵記憶部119に記憶された他のマスタ鍵を用いて、上記と同様に復号と判定を行う。

【0137】もし一時鍵の一致判定が成功したならば一致判定部283はゲート回路284を閉じ、一時鍵は、外部記憶装置112からインタフェース部を介して情報
40 処理装置111に送信される。この場合、上記のように情報処理装置111内の復号化部114にてこの一時鍵を用いて復号が行われる。

【0138】もし、この外部記憶装置112内のマスタ鍵記憶部119に記憶された全マスタ鍵について一時鍵の一致判定に失敗したならば、この外部記憶装置112ではこの暗号化された一時鍵を解くことはできない。この場合、一致判定部283はその旨を示す制御信号を発し、これが外部記憶装置112からインタフェース部を介して情報処理装置111に送信される。もちろん、こ

の場合、一時鍵は、情報処理装置111に送信されず、情報処理装置111では、暗号化データを復号化することはできない。

【0139】なお、図15の復号化部281と復号化部282とは、独立に設けても良いし、1つの復号化部を切り換えて使用するようにしても良い。図16は鍵の判定動作手順の一例を示すフローチャートである。

【0140】情報処理装置111側では、まず暗号化データ保持部116に格納されている暗号化データのヘッダ部161に含まれる $E_{Mki}(S_k)$ と $E_{Sk}(S_k)$ を、外部記憶装置112に送信する（ステップS21）。

【0141】外部記憶装置112側では、この $E_{Mki}(S_k)$ と $E_{Sk}(S_k)$ を受信する（ステップS22）。なお、情報処理装置111側からヘッダ部161全体を送信するようにした場合には、ヘッダ部161から $E_{Mki}(S_k)$ と $E_{Sk}(S_k)$ を取り出す。

【0142】次に、情報処理装置111から渡された $E_{Mki}(S_k)$ と、マスタ鍵記憶部119に記憶されているマスタ鍵 M_{kj} の組を選択する（ステップS23）。次に、マスタ鍵 M_{kj} を用いて、復号化部281にて、暗号化された一時鍵 $E_{Mki}(S_k)$ を復号して $S_k' = D_{Mkj}(E_{Mki}(S_k))$ を求める（ステップS24）。

【0143】次に、この $S_k' = D_{Mkj}(E_{Mki}(S_k))$ を用いて、復号化部282にて、マスタ鍵で暗号化された $E_{Sk}(S_k)$ を復号して $S_k'' = D_{Sk'}(E_{Sk}(S_k))$ を求める（ステップS25）。

【0144】次に、一致判定部283にて、 S_k' と S_k'' を比較し、一致しない場合（ステップS26）、情報処理装置111から渡された $E_{Mki}(S_k)$ と、マスタ鍵記憶部119に記憶されているマスタ鍵 M_{kj} の組でまだ選択していないものがあれば、（ステップS27）、ステップS23に戻る。

【0145】もし一致判定部283にて S_k' と S_k'' を比較し、一致した場合（ステップS26）、得られた一時鍵 $S_k (= S_k' = S_k'')$ を、情報処理装置111に送信する（ステップS28）。

【0146】情報処理装置111側では、一時鍵 S_k を受信すると（ステップS29）、暗号化されたデータ $E_{Sk}(\text{Data})$ を一時鍵 S_k で復号して平文のデータ Data を取り出す（ステップS30）。

【0147】なお、情報処理装置111から渡された $E_{Mki}(S_k)$ と、マスタ鍵記憶部119に記憶されているマスタ鍵 M_{kj} の組すべてについてステップS23～S26までの処理を試行し、そのすべてにおいて $S_k' = S_k''$ が得られなかった（ステップS26でNoとなった）場合、暗号化に使用したマスタ鍵が存在しないために一時鍵を復号化できなかった旨を示す制御信号を情報処理装置111に送信する。

【0148】なお、図17に、鍵判定システムの他の構

成を示す。図15との相違は、マスタ鍵 M_{kj} で E_{Mki} (S_k) を復号して $S_k' = D_{Mkj} (E_{Mki} (S_k))$ を求め、この S_k' を S_k' 自身で暗号化して $E_{Sk'} (S_k')$ を求め、 $E_{Mki} (S_k)$ と $E_{Sk'} (S_k')$ の一致により検証を行う点である。この処理手順のフローチャートは、図16のステップS25の処理で、 S_k' を S_k' 自身で暗号化して $E_{Sk'} (S_k')$ を求める点、ステップS26で $E_{Mki} (S_k)$ と $E_{Sk'} (S_k')$ を比較する点以外は、図16と同様である。

【0149】なお、図17の復号化部281と暗号化部285の処理が同内容になる暗号方式を採用する場合、復号化部281と暗号化部285とは、独立に設けても良いし、1つの回路を切り換えて使用するようにしても良い。

【0150】前述したように、暗号化されたデータ E_{Sk} (Data) を解読するためには、 $E_{Mki} (S_k)$ を解読して一時鍵を取り出す必要がある。復号側で該当するマスタ鍵を所有する場合にのみデータDataを取り出すことができる。例えば、暗号化データのヘッダ部に $E_{Mk1} (S_k)$ 、 $E_{Mk2} (S_k)$ 、 $E_{Mk3} (S_k)$ が含まれる場合には、 M_{k1} 、 M_{k2} 、 M_{k3} のいずれかのマスタ鍵を持つものが、平文のデータDataを得ることができる。

【0151】つまり、このDataを M_{k1} 、 M_{k2} 、 M_{k3} のいずれかのマスタ鍵を持つユーザによって共有し、他のユーザには内容を秘匿することができる。また、ヘッダ部に含まれる一時鍵自身で暗号化された一時鍵 $E_{Sk} (S_k)$ をもとにして、復号した一時鍵の検証を行い、検証を通過しない場合には復号化の処理が実行されない。異なる鍵を用いて誤って暗号化されたデータを破壊するようなトラブルを回避することができる。

【0152】さらに、1つの暗号化データを解読可能とするマスタ鍵の数にかかわらず、上記検証のために不可する情報は、一時鍵自身で暗号化された一時鍵のただ1つのみで良いという利点がある。

【0153】また、以上のような本実施形態によれば、一時鍵の暗号化、復号化は、情報処理装置の外部で行われるため、マスタ鍵と情報処理装置が分離され、マスタ鍵を安全に扱うことができる。例えば、不正な第三者が本情報処理装置にアクセスしたとしても、マスタ鍵は情報処理装置内には存在しないので、マスタ鍵を盗用されることはない。

【0154】また、データの暗号化および復号化は、暗号化する度に生成される一時鍵を用いて行うので、ある暗号化データの一時鍵が解読された場合でも、他の暗号化データをその一時鍵で解読することはできない。

【0155】また、データを暗号化する一時鍵を変更せずに、マスタ鍵だけを変更する場合、ヘッダ部に所望のマスタ鍵で暗号化した一時鍵を追加し、あるいはヘッダ部から該当するマスタ鍵で暗号化した一時鍵を削除す

ば良く、データを再暗号化する必要がない。

【0156】また、暗号方式として任意の方式を用いる場合、暗号方式の識別子を暗号化データのヘッダ部に付加しておけば、暗号方式を自由に選択することが可能である。

【0157】なお、暗号側で用いる処理機能付き外部記憶装置1と復号側で用いる処理機能付き外部記憶装置11とを1つの外部記憶装置で共用する場合、暗号化に用いるマスタ鍵と復号化に用いるマスタ鍵を同一にしても良いし、暗号化にのみ使用可能なマスタ鍵記憶部と復号化にのみ使用可能なマスタ鍵記憶部を設け、それぞれに所望のマスタ鍵を記憶させるようにしても良い。

【0158】ここで、本実施形態に係る情報処理システムの利用例について述べる。例えば、前述した暗号側と復号側の機能を兼ね備える情報処理装置を複数台、LANなどに接続する。また、このLANにはファイルを蓄積・管理するファイル管理装置が接続されているものとする。各情報処理装置のユーザは、前述のようにマスタ鍵を保管してある処理機能付き外部記憶装置を用いて、暗号化されたデータを含むファイルを作成し、LANを介して上記のファイル管理装置に保存する。その際、そのファイルのヘッダに所望のユーザのマスタ鍵により暗号化された一時鍵を付加しておけば、当該暗号化ファイルは、該当するユーザであればいずれも解読することができる。このようにして、暗号化ファイルを安全に共有するシステムを構築することができる。

【0159】もちろん、1つのスタンドアローンの情報処理装置を複数ユーザで共用しており、この情報処理装置に内蔵のハードディスク装置に格納されるファイルを複数ユーザで共有するような場合にも、本発明は適用可能である。

【0160】ところで、暗号化対象であるデータの暗号方式と一時鍵の暗号方式の少なくとも一方に、RSAなどの所望の公開鍵暗号方式を用いても良い。例えば、一時鍵の暗号方式に所望の公開鍵暗号方式を用いる場合、暗号化する際、マスタ鍵として対象ユーザの公開鍵を使用し、復号化する際、マスタ鍵として自身の秘密鍵を使用する。また、例えば、暗号化対象であるデータの暗号方式に、暗号化鍵と復号化鍵が異なる暗号方式を用いる場合、暗号化する際、一時鍵として暗号化鍵と復号化鍵の対を生成し、暗号化鍵でデータを暗号化するとともに、復号化鍵を暗号化し、これをヘッダ部に格納する。

【0161】また、マスタ鍵を格納する外部記憶装置を使用しないならば、以下のようにマスタ鍵を生成し使用する。まず、暗号化、復号化を行う情報処理装置にパスワードやID番号を入力することにより、一方向性関数等を用いて、暗号化、復号化の鍵を生成するマスタ鍵生成部を用意する。このマスタ鍵生成部では、個人やグループのパスワードやID番号を入力することにより、異なるマスタ鍵を各々に対し生成する。これらのマスタ鍵

は、上記した方法と同じように、暗号化装置では一時鍵を暗号化するときを使用し、復号化装置では一時鍵を復号するとき使用する。

【0162】以上の各構成は、ハード・ワイヤードで形成することも、相当するプログラムをCPUで実行させる形で実現することも可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0163】以上、上記した第3、第4実施形態によれば、所定の一時鍵で暗号化されたデータに、所定のマスタ鍵で暗号化された一時鍵と、一時鍵自身で暗号化された一時鍵を付加するので、該当するマスタ鍵を持つユーザのみ鍵の検証と暗号化されたデータの復号化を行うことができ、その他のユーザには内容を秘匿することができる。

【0164】また、一時鍵自身で暗号化した一時鍵を用いて鍵の検証を行いながら復号化を行うので、正当ではないマスタ鍵の誤用などによる復号時のデータの破壊を避けることができる。しかも、一時鍵自身で暗号化された一時鍵を付加するだけで、すべてのマスタ鍵について

鍵の検証を行うことができる。

【0165】従って、例えば、個人やグループなどの複数のユーザで共有するデータを、暗号化した形で安全に保存できるようになる。また、一時鍵の暗号化、復号化は、情報処理装置の外部で行われるため、マスタ鍵と情報処理装置が分離され、マスタ鍵を安全に扱うことができる。例えば、不正な第3者が本情報処理装置にアクセスしたとしても、マスタ鍵は情報処理装置内には存在しないので、マスタ鍵を盗用されることはない。

【0166】図18は、本発明の第5実施形態として、鍵の判定方法を一般化した場合の鍵判定システムの構成を示す図である。第5実施形態に係る鍵判定システムでは、一時鍵 S_k をマスター鍵 M_k で暗号化して得られるデータを $M_k(S_k)$ として入力するとともに、後述する複数のチェック関数の任意の一つをチェックデータとして選択的に入力する。判定部300はこれら2つのデータに基づいて、マスター鍵を用いた所定の暗号化及び／または復号処理を行なうことにより、当該マスター鍵が正しいか否かを判定し、この判定結果(YES/NO)を出力するとともに、復号された一時鍵 S_k を出力する。

【0167】図19は鍵判定システムに対する入力となり得る複数のチェック関数を区別して示すテーブルを示すものである。チェック関数 $X(a)$ とは鍵 a を鍵 X で暗号化して得られるデータを意味し、 $X^{-1}(a)$ は鍵 a を鍵 X で復号して得られるデータを意味し、 X^2

(a)は鍵 a を鍵 X で2回暗号化して得られるデータを意味する。また、 h はハッシュ関数を意味し、 $||$ は2つの鍵を並べることを意味し、 $+$ は加算を意味し、 d は複数の人によって共有される共有データであり、 d^* は

時変、すなわち、暗号化あるいは復号処理を行なう毎に異なる共有データを表す。

【0168】まず、 M_k の暗号化あるいは復号を行なう場合に用いられる各チェック関数について説明する。チェック関数が M_k と S_k を共に含む場合は、 $S_k(M_k)$ と $S_k^{-1}(M_k)$ が存在し、いずれも含まない場合は $h(M_k || S_k)$ が存在する。また、チェック関数が M_k のみか、あるいは M_k と他のデータを含む場合には、 $M_k(M_k)$ 、 $M_k^{-1}(M_k)$ 、 $M_k(M_k + d^*)$ 、 $M_k^{-1}(M_k + d^*)$ の4通りが存在し、含まない場合は $M_k(d^*)$ 、 $M_k^{-1}(d^*)$ 、 $h(M_k)$ の3通りが存在する。また、チェック関数が S_k のみか、あるいは S_k と他のデータについてのチェック関数は存在しない。

【0169】次に、 S_k の暗号化あるいは復号を行なう場合に用いられる各チェック関数について説明する。チェック関数が M_k と S_k を共に含む場合は、 $M_k^2(S_k)$ と $M_k^{-1}(S_k)$ が存在し、含まない場合は $h(M_k || S_k)$ が存在する。また、チェック関数が M_k のみか、あるいは M_k と他のデータについてのチェック関数は存在しない。また、チェック関数が S_k のみか、あるいは S_k と他のデータを含む場合は $S_k(S_k)$ 、 $S_k^{-1}(S_k)$ が存在し、含まない場合は $S_k(d)$ 、 $S_k^{-1}(d)$ 、 $h(S_k)$ の3通りが存在する。

【0170】図20は、チェック関数として、 $S_k(M_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路301と暗号化回路302と一致判定部303とゲート304とを具備する。復号回路301、暗号化回路302、一致判定部303の動作は前記した通りである。矢印はマスター鍵 M_k の入力を意味する。また、ゲート304はデータを出力するかどうかを制御するのに用いられる。これらの説明は以下で述べるチェック関数にも適用されるものとする。

【0171】図21は、チェック関数として、 $S_k^{-1}(M_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路305、306と、一致判定部307と、ゲート308を具備する。

【0172】図22は、チェック関数として、 $M_k(M_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路309と一致判定部310と暗号化回路311とゲート312とを具備する。

【0173】図23は、チェック関数として、 $M_k^{-1}(M_k)$ が入力される場合の鍵判定システムの構成を示す図であり、ゲート313と復号回路314と一致判定部315と復号回路316とを具備する。

【0174】図24は、チェック関数として、 d^* 及び $M_k(M_k + d^*)$ が入力される場合の鍵判定システムの構成を示す図であり、ゲート317と復号回路318と一致判定部319と暗号化回路320と加算回路321とを具備する。

【0175】図25は、チェック関数として、 d^* 及び $M_k^{-1}(M_k + d^*)$ が入力される場合の鍵判定システムの構成を示す図であり、ゲート322と復号回路323と一致判定部324と復号回路325と加算回路326とを具備する。

【0176】図26は、チェック関数として、 $h(M_k || S_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路327と連結部328とハッシュ関数(h)329とゲート330と一致判定部331とを具備する。

【0177】図27は、チェック関数として、 d^* 及び $M_k(d^*)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路332と一致判定部333とゲート334と復号回路335とを具備する。

【0178】図28は、チェック関数として、 d^* 及び $M_k^{-1}(d^*)$ が入力される場合の鍵判定システムの構成を示す図であり、暗号化回路336と一致判定部337とゲート338と復号回路339とを具備する。

【0179】図29は、チェック関数として、 $h(M_k)$ が入力される場合の鍵判定システムの構成を示す図であり、一致判定部340とハッシュ関数(h)341とゲート342と復号回路343とを具備する。

【0180】図30は、チェック関数として、 $M_k^2(S_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路344と暗号化回路345とゲート347と一致判定部346とを具備する。

【0181】図31は、チェック関数として、 $M_k^{-1}(S_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路348と一致判定部349と暗号化回路350とを具備する。

【0182】図32(a)、(b)は、チェック関数として、 $S_k(S_k)$ が入力される場合の鍵判定システムの構成を示す図である。図32Aは復号回路360と暗号化回路361と一致判定部362とゲート363とを具備し、図32Bは復号回路364、365と一致判定部366とゲート367とを具備する。

【0183】図33(a)、(b)は、チェック関数として、 $S_k^{-1}(S_k)$ が入力される場合の鍵判定システムの構成を示す図である。図33Aは復号回路368、369と一致判定部370とゲート371とを具備し、図33Bは復号回路372と暗号化回路373と一致判定部374とゲート375とを具備する。

【0184】図34は、チェック関数として、 d 及び $S_k(d)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路376、377と一致判定部378とゲート379とを具備する。

【0185】図35は、チェック関数として、 d 及び $S_k^{-1}(d)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路380と暗号化回路381と一致判定部382とゲート383とを具備する。

【0186】図36は、チェック関数として $h(S_k)$ が入力される場合の鍵判定システムの構成を示す図であり、復号回路384とハッシュ関数(h)385と一致判定部386とゲート387とを具備する。

【0187】図37は、第5実施形態の鍵判定システムをDVD(デジタルビデオディスク)に応用した例を説明するための図である。送信側は一時鍵 S_k を複数の暗号化回路500-1~500-nの各々に入力して異なるマスター鍵 $M_{k1} \sim M_{kn}$ を用いて暗号化して同時に送信する。このとき、一時鍵 S_k を自身の鍵 S_k で暗号化したデータも同時に送信する。

【0188】受信側では複数の復号回路501-1~501-nの各々に送信時に用いたマスター鍵 $M_{k1} \sim M_{kn}$ を入力すれば S_k が得られる。このとき、例えば復号回路501-3において M_{k3} とは異なるマスター鍵 M_{k3}' を用いて復号した場合は S_k とは異なる一時鍵 S_k' が得られるので、比較部503で同じ S_k' で暗号化して得られる S_k' (S_k') を送信側から送られてきた S_k (S_k) と比較しても一致しないので S_k が出力されずエラーとなる。このようにしてマスター鍵の真偽判定が行われる。

【0189】図38は、第5実施形態の鍵判定システムを電子メールに応用した例を説明するための図である。電子メールのヘッダ400には、一時鍵 S_k を複数の異なるマスター鍵 $M_{k1} \sim M_{kn}$ で暗号化したデータ $M_{k1}(S_k) \sim M_{kn}(S_k)$ と、 S_k を同じ S_k で暗号化した $S_k(S_k)$ とを記録し、ボディ401には、本文を S_k で暗号化した S_k (本文) を記録して、各 $M_{k1} \sim M_{kn}$ に対応する宛先1~nに同報的に送信する。ここで受信側としての宛先1は所持している M_{k1} を用いて復号して S_k を取り出し、これを同じ S_k で暗号化したものと、受信した $S_k(S_k)$ とを比較し、一致した場合には S_k が得られるのでこの S_k を用いて復号することにより本文を得ることができる。

【0190】ここで、不正な第3者が自身のマスター鍵で復号しようとしても比較結果が一致しないので S_k を正しく復号できず本文が知られてしまうことはない。図39は、第5実施形態の鍵判定システムをCATVに応用した例を説明するための図である。

【0191】第1の例は受信側が鍵のデータベースを有している例である。送信側としての放送局600がある特定地域の受信局に放送内容を送る場合に、この放送内容を S_k で暗号化したデータ S_k (内容) と、 S_k を M_k で暗号化したデータ $M_k(S_k)$ と、 S_k を S_k で暗号化したデータ $S_k(S_k)$ と送信する。受信局のデコーダ601は複数の鍵からなる鍵データベース602を有しており、この鍵データベース602から受信した M_k に一致するものを鍵セレクト部603で選択して、選択された鍵を用いて復号することにより S_k を得る。次にこの S_k を S_k 自身で暗号化したものと、送られてき

た S_k (S_k) とを比較して一致したときに S_k を復号回路604に出力する。復号回路604はこの S_k を用いて受信した S_k (内容) を復号して内容を取り出してTV605の画面に表示する。ここで、不正な第3者が自身のマスター鍵で復号しようとしても比較結果が一致しないので S_k を正しく復号できず放送内容が見られてしまうことはない。

【0192】上記した構成において、鍵データベース602に、例えば受信局がその移転前に用いた鍵と、移転後に用いている鍵を記憶しておけば、移転した後もその鍵が選択されるのでデコーダ601の構成を変更することなしに正常に内容を復号することができる。

【0193】次に第2の例を説明する。第2の例の基本的構成は第1の例と同様であるが、この例では送信側としての放送局600と受信局の双方が鍵のデータベースを有している。放送局600は鍵データベースの中から1つの鍵を選択して送信する。受信局のデコーダ601は鍵データベース602の中から対応する1つの鍵を選択して復号する。この場合、放送局600から送信される鍵は M_k 、 S_k 共に送信ごとに逐次変更され、しかも、放送局600はこの変更についての情報は受信局には送信しないようにする。このようにすれば第1の例の効果に加えて、安全性をより向上することができる。

【0194】次に第3の例を説明する。第3の例の基本的構成は第1の例と同じであり、この場合も受信局が鍵のデータベースを有しているものとする。ここでは、鍵が漏洩してしまつて新たな鍵に変更したい場合や、現在の鍵のバージョンを新たなバージョンに変更したい場合に対処するために、あらかじめ新旧バージョンの鍵を鍵のデータベース602に含めておく。このようにすれば、デコーダ601の構成を変更することなしに、変更後の新しい鍵が送られてきても正常に復号することができる。

【0195】

【発明の効果】本発明によれば、たとえ装置が盗難されたり分解されたりしても、内部に記憶された機械情報を保護することができる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することができる。

【0196】また、本発明によれば、複数のユーザで共有するデータを、効率的かつ安全に暗号化した形で保存できる情報処理装置、情報処理システム、情報処理方法、記録媒体、及び鍵の判定方法及び装置を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、暗号化を行なう場合の装置構成を示す図である。

【図2】暗号化を行った後の携帯型情報処理システムの構成の変更を示す図である。

【図3】本発明の第1実施形態に係る情報処理システムが適用される携帯型情報処理システムにおいて、復号化を行なう場合の装置構成を示す図である。

【図4】本発明の第2実施形態に係る鍵の判定を実現するための鍵判定システムの構成を示す図である。

【図5】図4に示す装置構成を簡略化した構成を示す図である。

【図6】図5に示す構成の変形例を示す図である。

【図7】図5に示す構成の他の変形例を示す図である。

10 【図8】本発明の第3実施形態に係る情報処理システム(暗号側)の構成を示す図である。

【図9】図8の外部記憶装置の内部構成の一例を示す図である。

【図10】マスタ鍵選択指示部を含めた情報処理システムの構成を示す図である。

【図11】鍵情報テーブルの一例を示す図である。

【図12】鍵選択指示用画面の一例を示す図である。

【図13】暗号化の動作手順の一例を示すフローチャートである。

20 【図14】本発明の第3実施形態に係る情報処理システム(復号側)の構成を示す図である。

【図15】本発明の第4実施形態に係る鍵の判定を実現するための鍵判定システムの構成を示す図である。

【図16】鍵の判定動作手順の一例を示すフローチャートである。

【図17】鍵判定システムの他の構成を示す図である。

【図18】本発明の第5実施形態として、鍵判定方法を一般化した場合の鍵判定システムの構成を示す図である。

30 【図19】鍵判定システムに対する入力となり得る複数のチェック関数を区分けして示すテーブルである。

【図20】チェック関数として、 S_k (M_k) が入力された場合の鍵判定システムの構成を示す図である。

【図21】チェック関数として、 S_k^{-1} (M_k) が入力された場合の鍵判定システムの構成を示す図である。

【図22】チェック関数として、 M_k (M_k) が入力された場合の鍵判定システムの構成を示す図である。

【図23】チェック関数として、 M_k^{-1} (M_k) が入力された場合の鍵判定システムの構成を示す図である。

40 【図24】チェック関数として、 d^* 及び M_k ($M_k + d^*$) が入力された場合の鍵判定システムの構成を示す図である。

【図25】チェック関数として、 d^* 及び M_k^{-1} ($M_k + d^*$) が入力された場合の鍵判定システムの構成を示す図である。

【図26】チェック関数として、 $h(M_k || S_k)$ が入力された場合の鍵判定システムの構成を示す図である。

50 【図27】チェック関数として、 d^* 及び M_k (d^*) が入力された場合の鍵判定システムの構成を示す図であ

る。

【図28】チェック関数として、 d^* 及び $M_k^{-1}(d^*)$ が入力された場合の鍵判定システムの構成を示す図である。

【図29】チェック関数として、 $h(M_k)$ が入力された場合の鍵判定システムの構成を示す図である。

【図30】チェック関数として、 $M_k^2(S_k)$ が入力された場合の鍵判定システムの構成を示す図である。

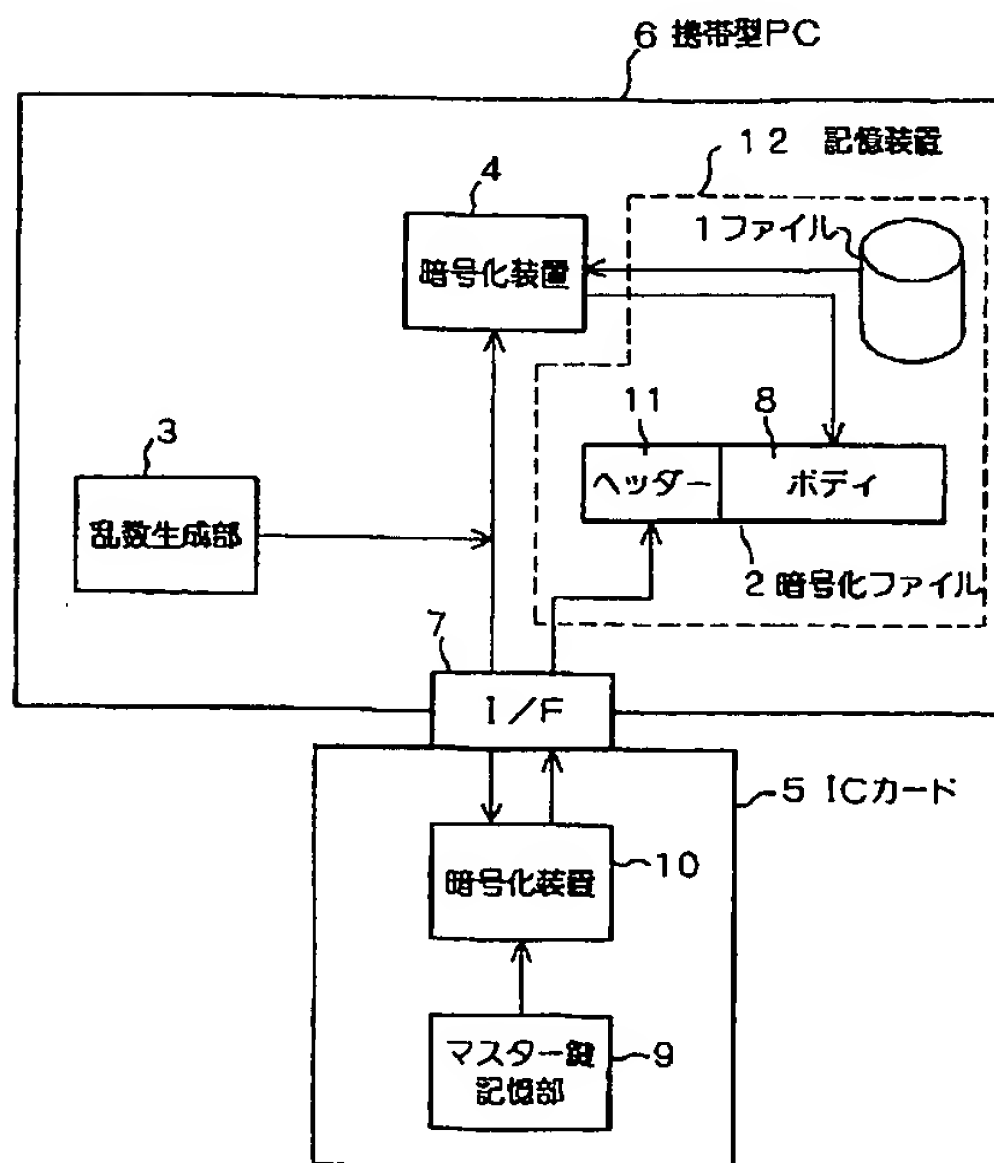
【図31】チェック関数として、 $M_k^{-1}(S_k)$ が入力された場合の鍵判定システムの構成を示す図である。

【図32】チェック関数として、 $S_k(S_k)$ が入力された場合の鍵判定システムの構成を示す図である。

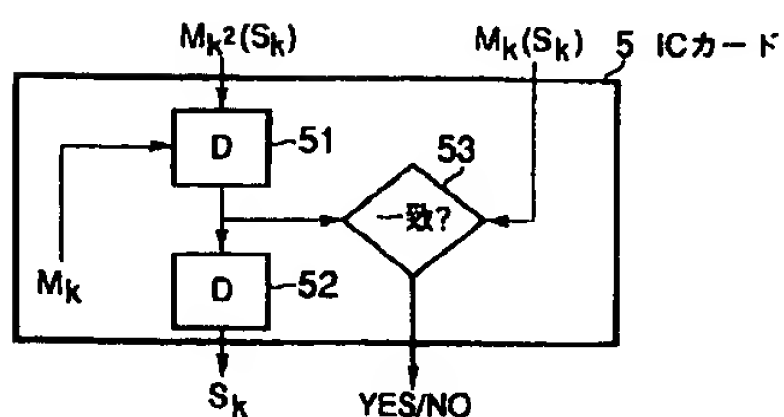
【図33】チェック関数として、 $S_k^{-1}(S_k)$ が入力された場合の鍵判定システムの構成を示す図である。

【図34】チェック関数として、 d 及び $S_k(d)$ が入力された場合の鍵判定システムの構成を示す図である。

【図1】



【図5】



【図35】チェック関数として、 d 及び $S_k^{-1}(d)$ が入力された場合の鍵判定システムの構成を示す図である。

【図36】チェック関数として $h(S_k)$ が入力された場合の鍵判定システムの構成を示す図である。

【図37】本発明の第5実施形態の鍵判定システムの第1の応用例を説明するための図である。

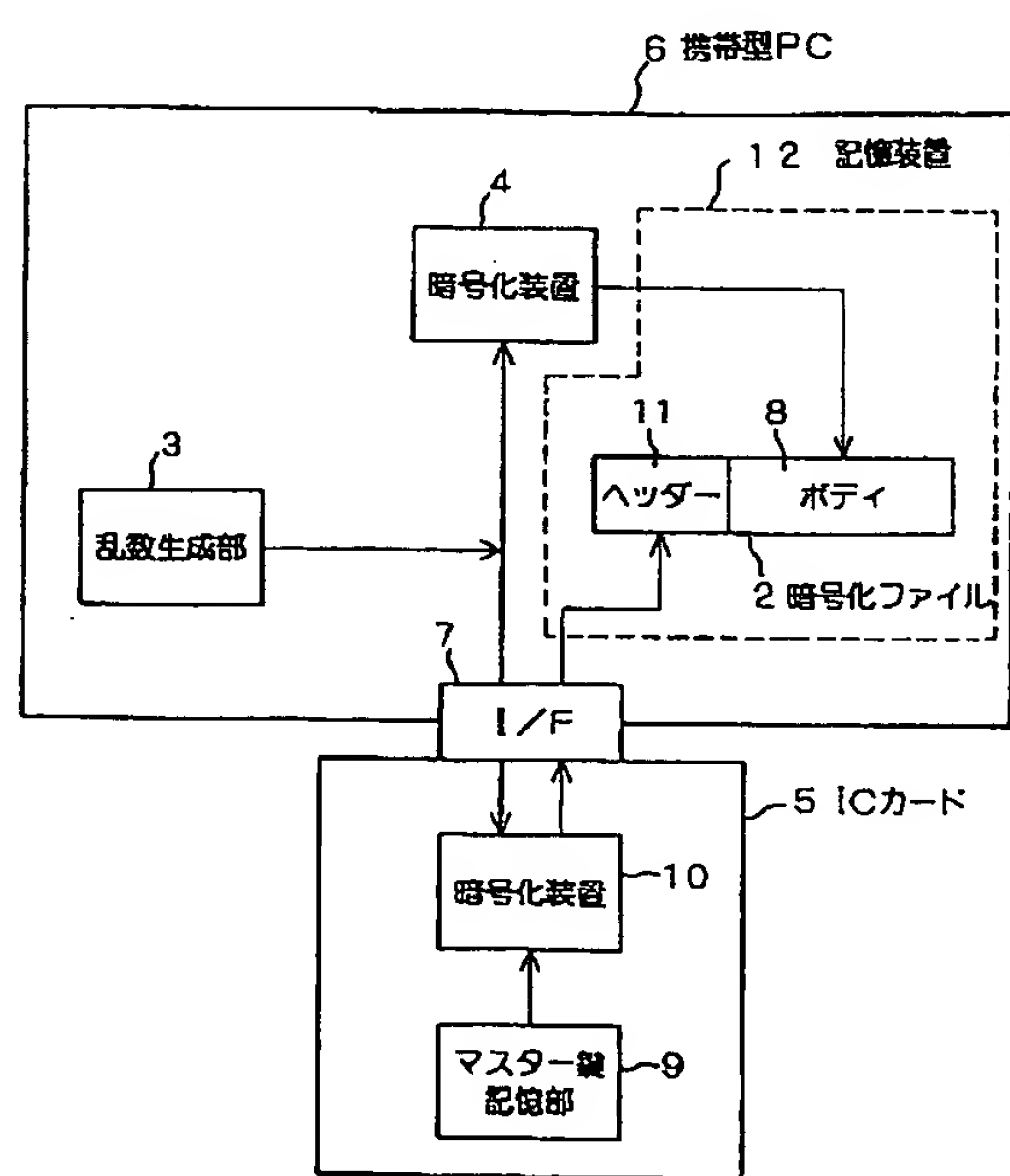
【図38】本発明の第5実施形態の鍵判定システムの第2の応用例を説明するための図である。

10 【図39】本発明の第5実施形態の鍵判定システムの第3の応用例を説明するための図である。

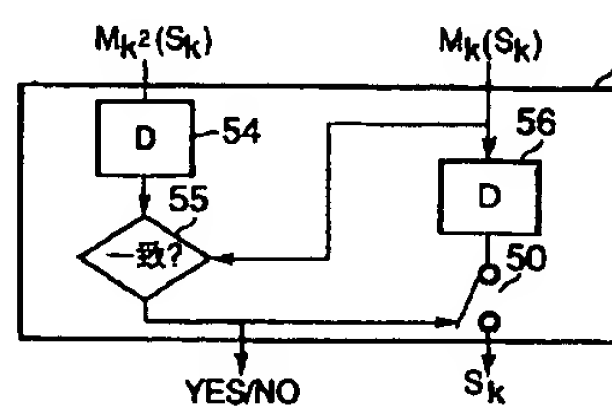
【符号の説明】

1…ファイル、2…暗号化ファイル、3…乱数生成部、4…暗号化装置、5…ICカード、6…携帯型PC、7…I/F、8…ボディ、9…マスター鍵記憶部、10…暗号化装置、11…ヘッダー、12…記憶装置。

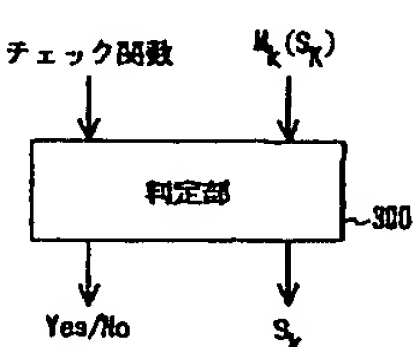
【図2】



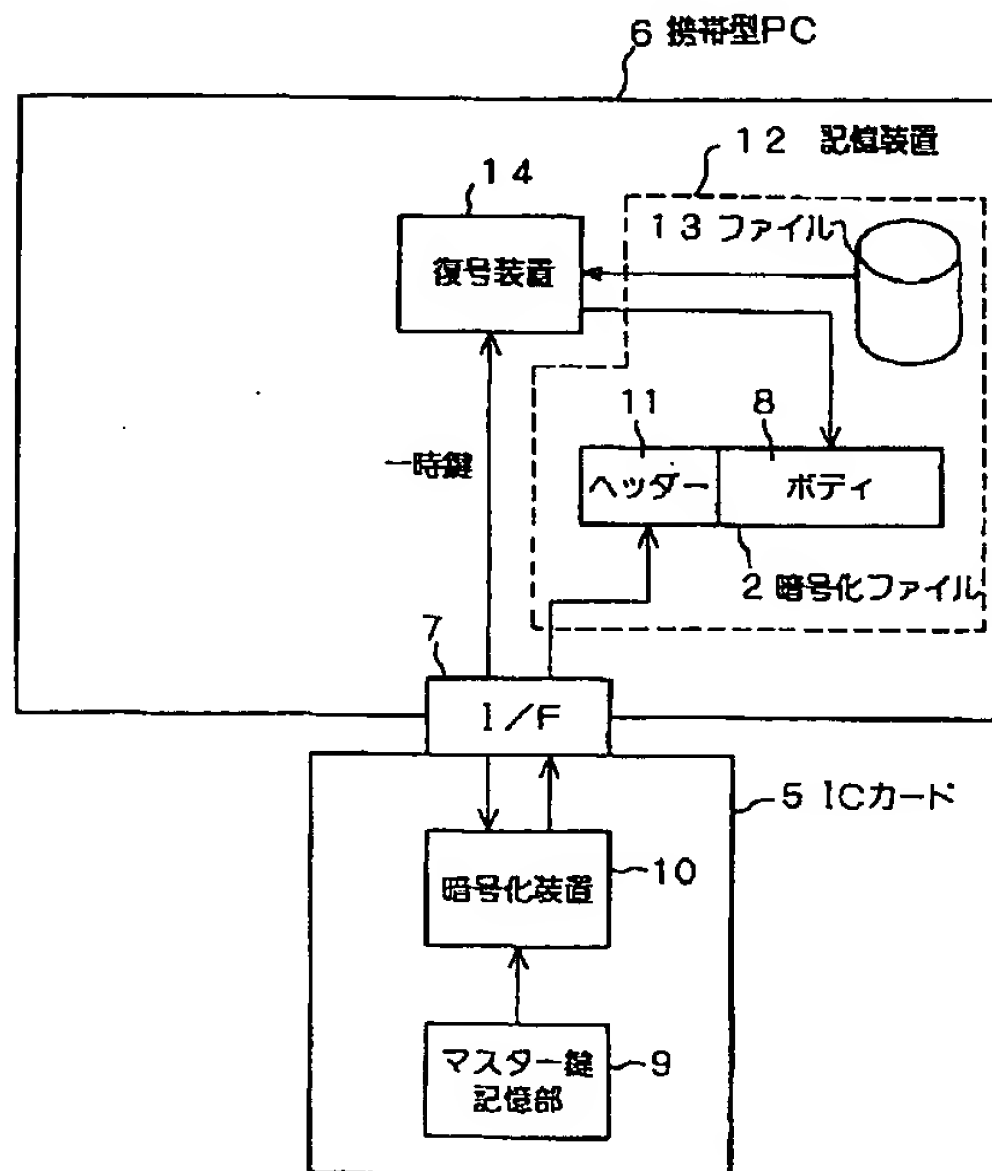
【図6】



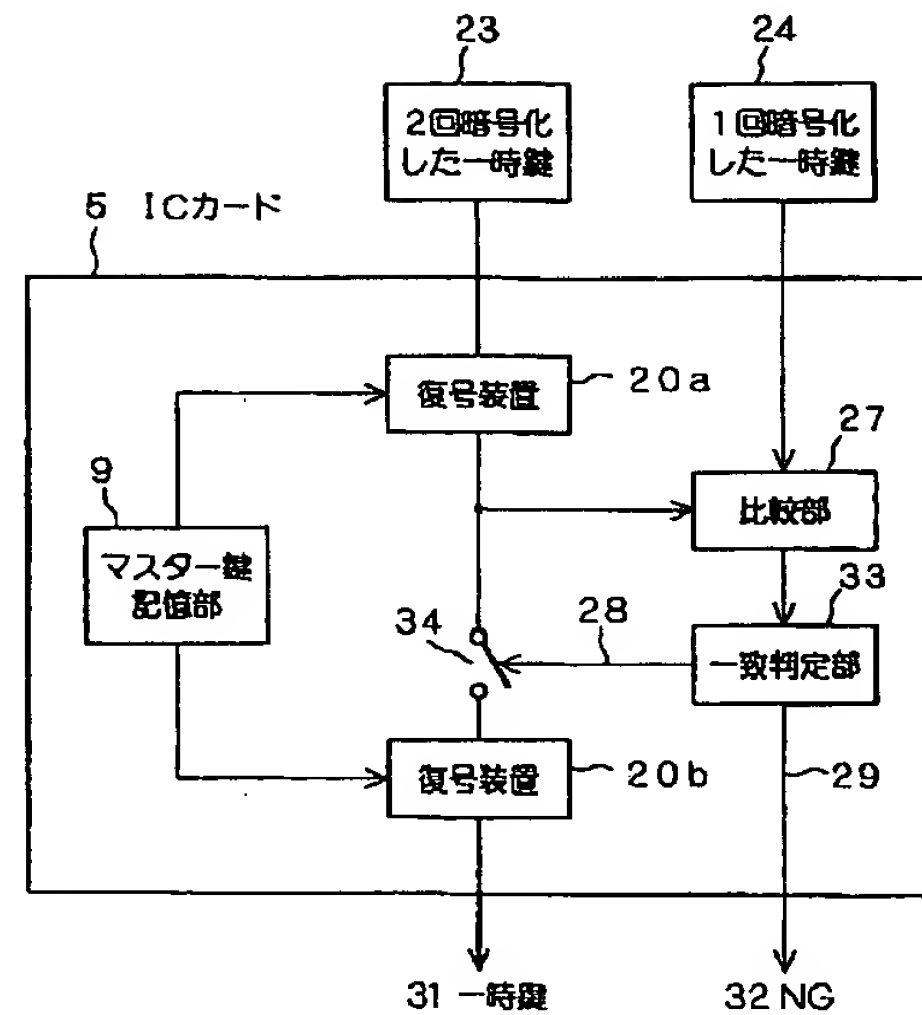
【図18】



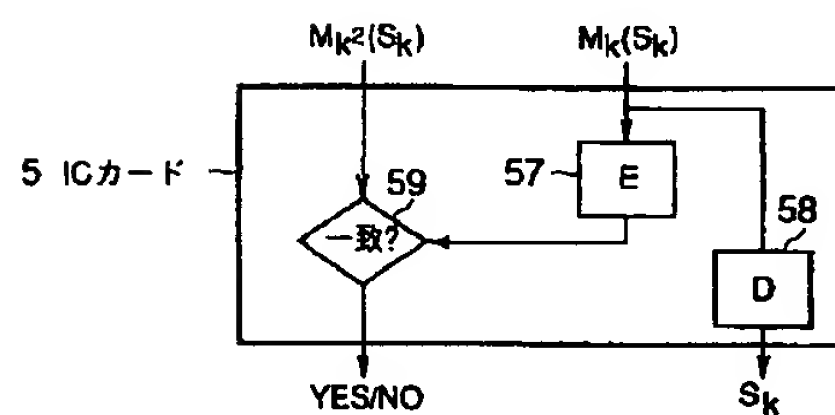
【图 3】



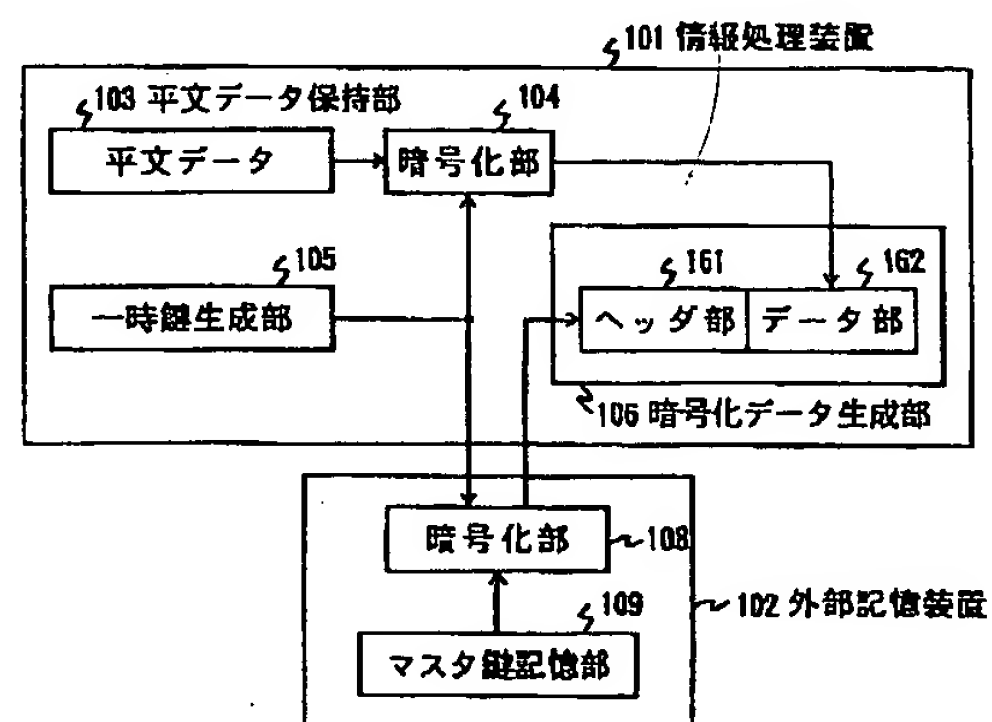
【図4】



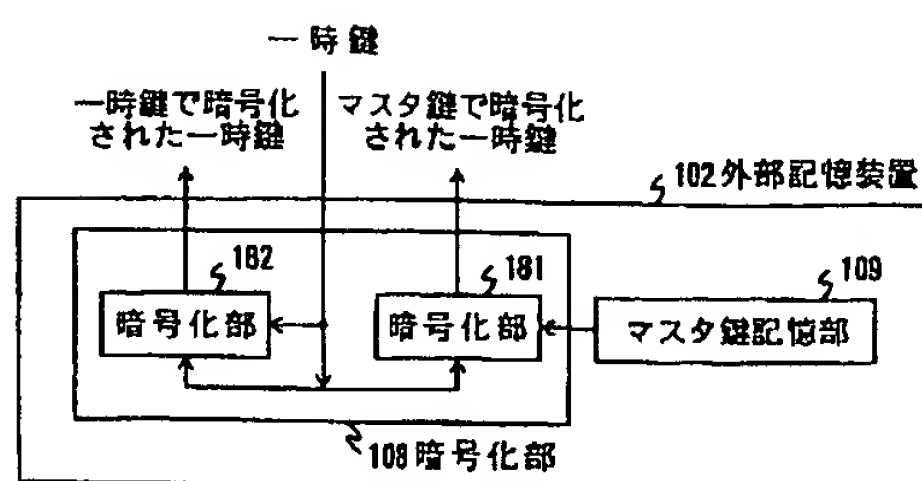
【图 7】



【图 8】



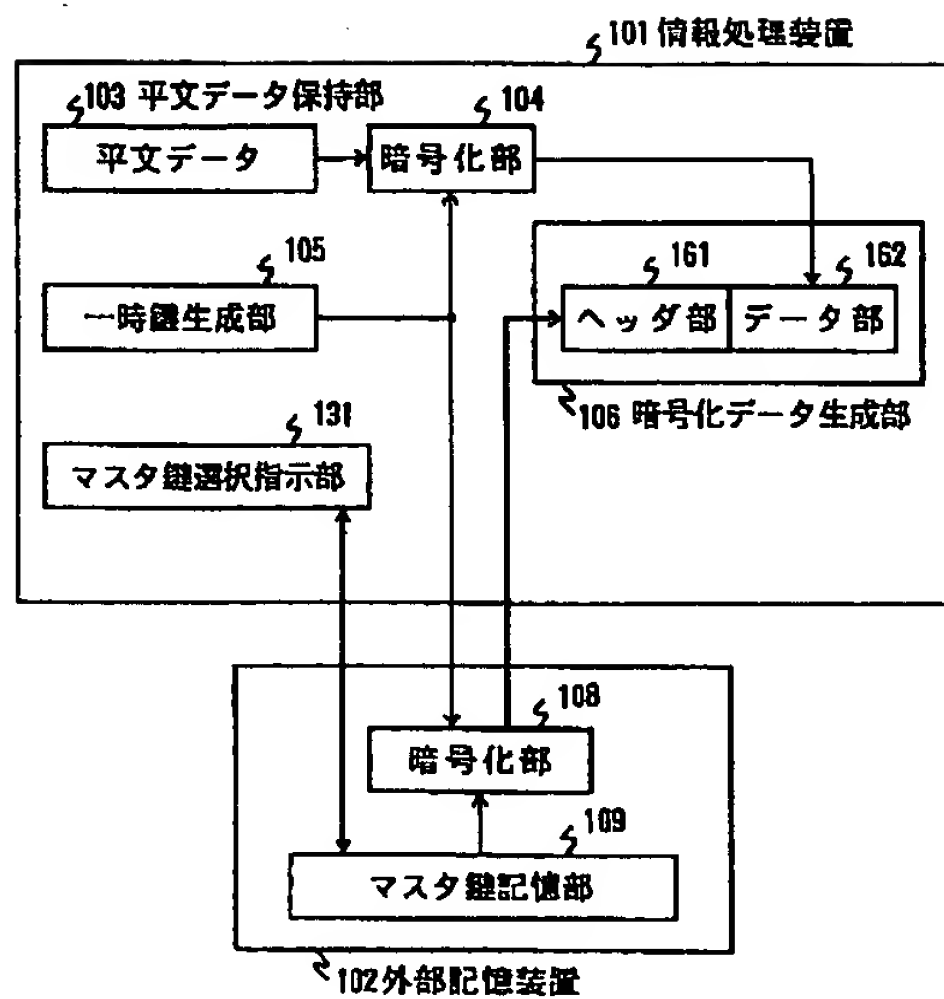
【图 9】



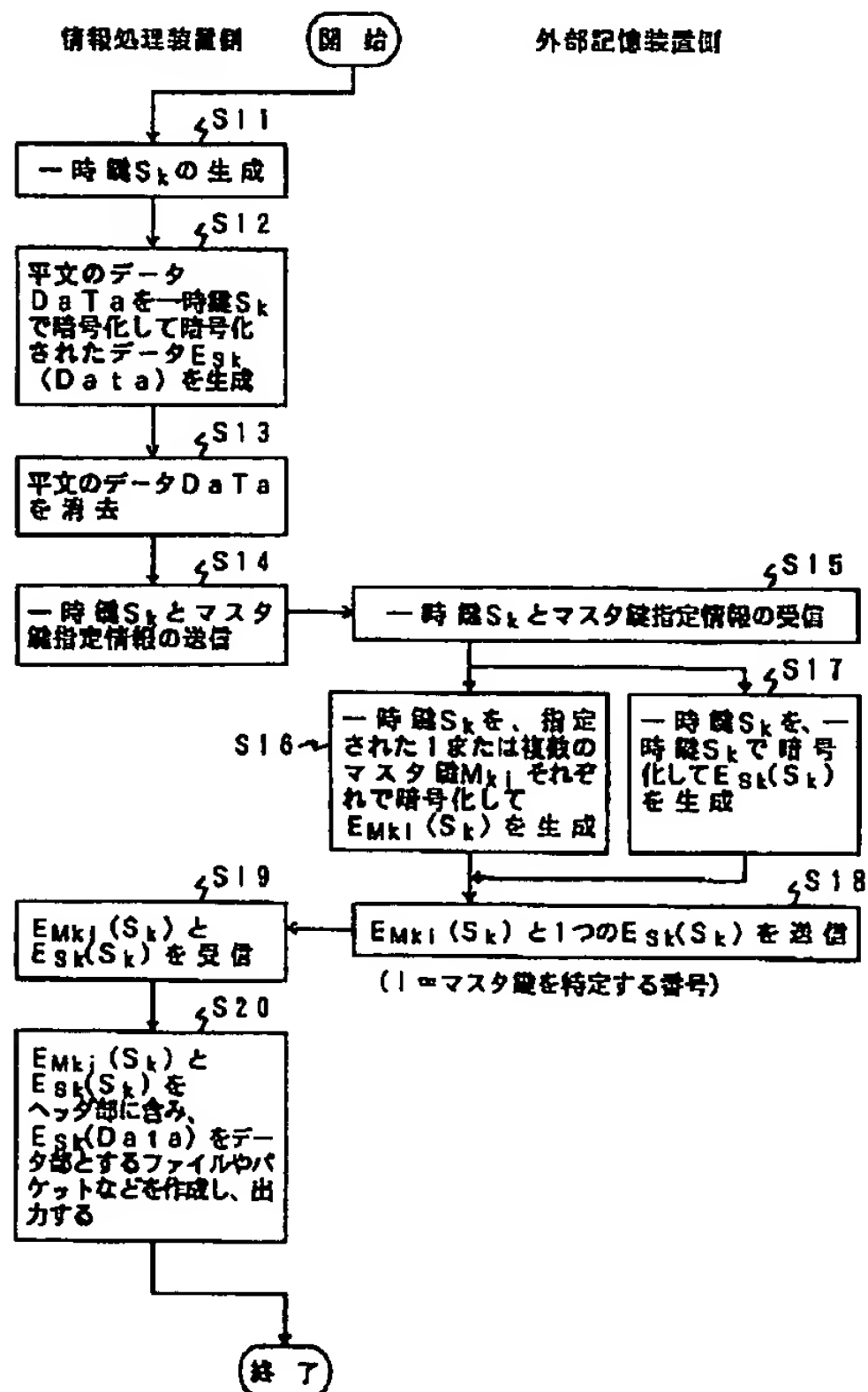
【图 1 1】

鍵 I D	鍵データ	ユーザ情報
⋮	⋮	⋮

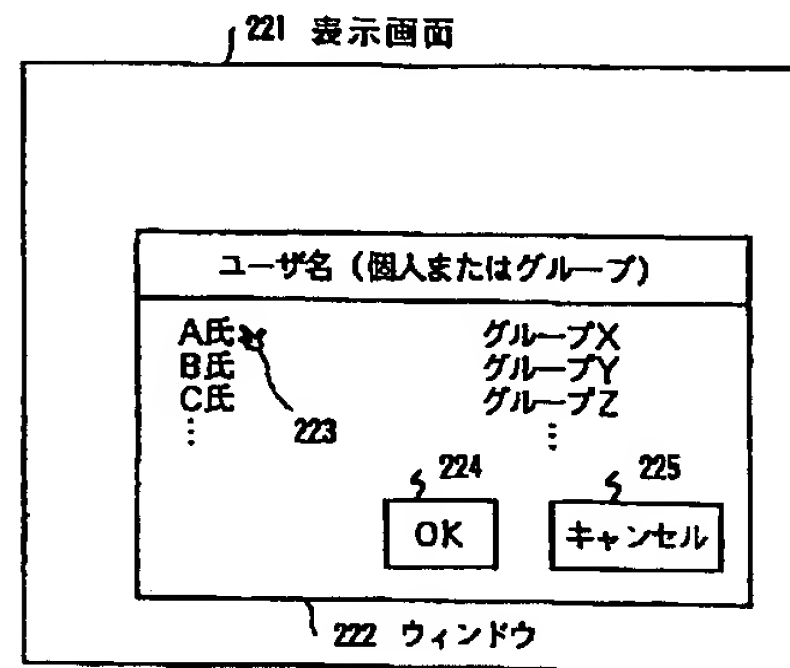
【図10】



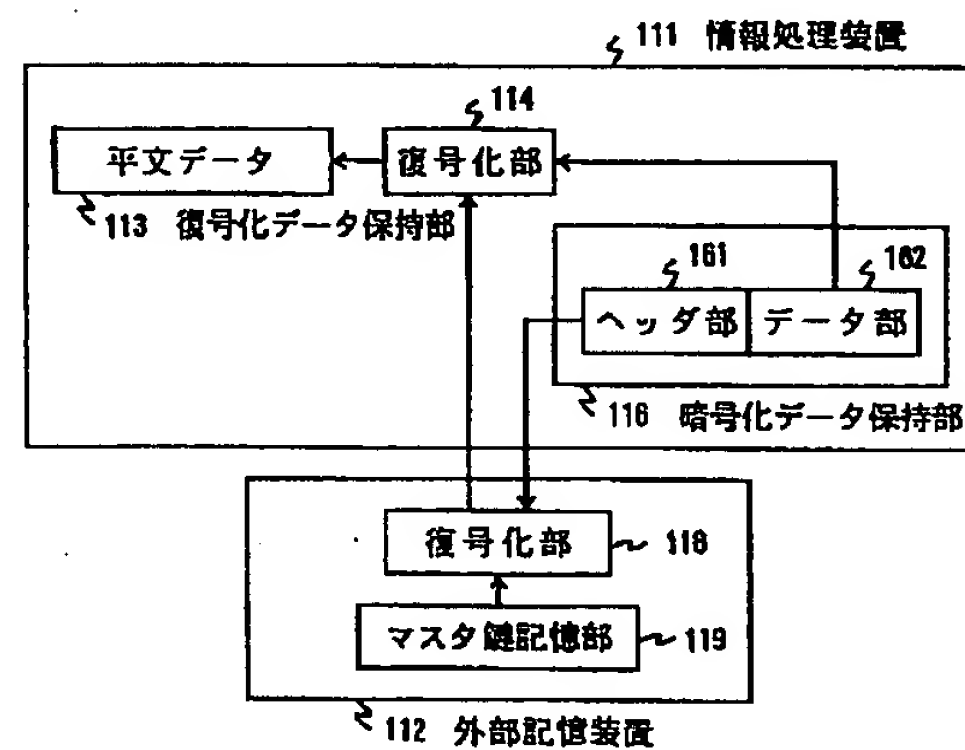
【図13】



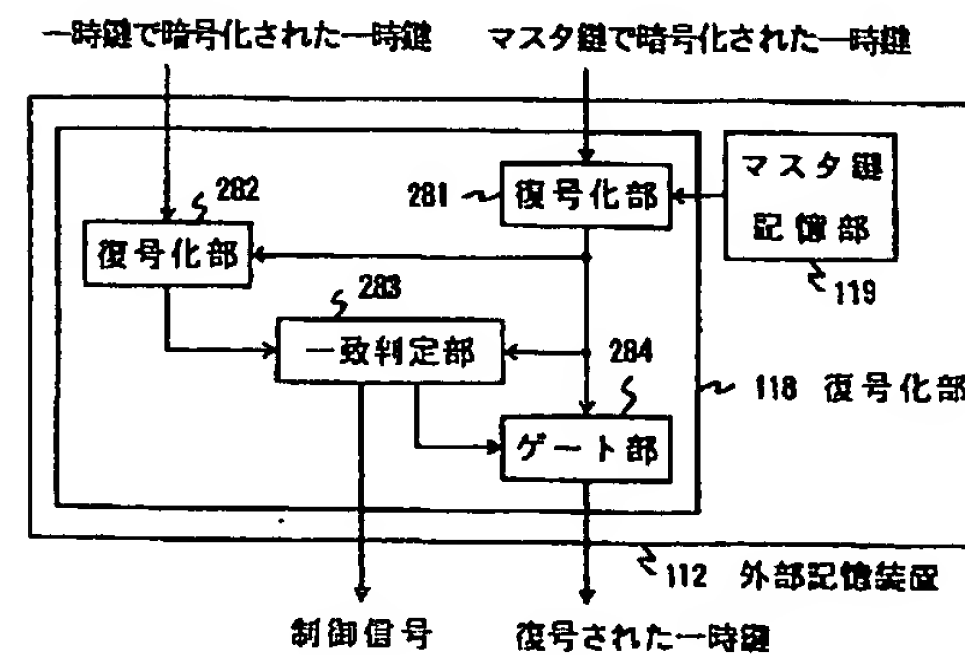
【図12】



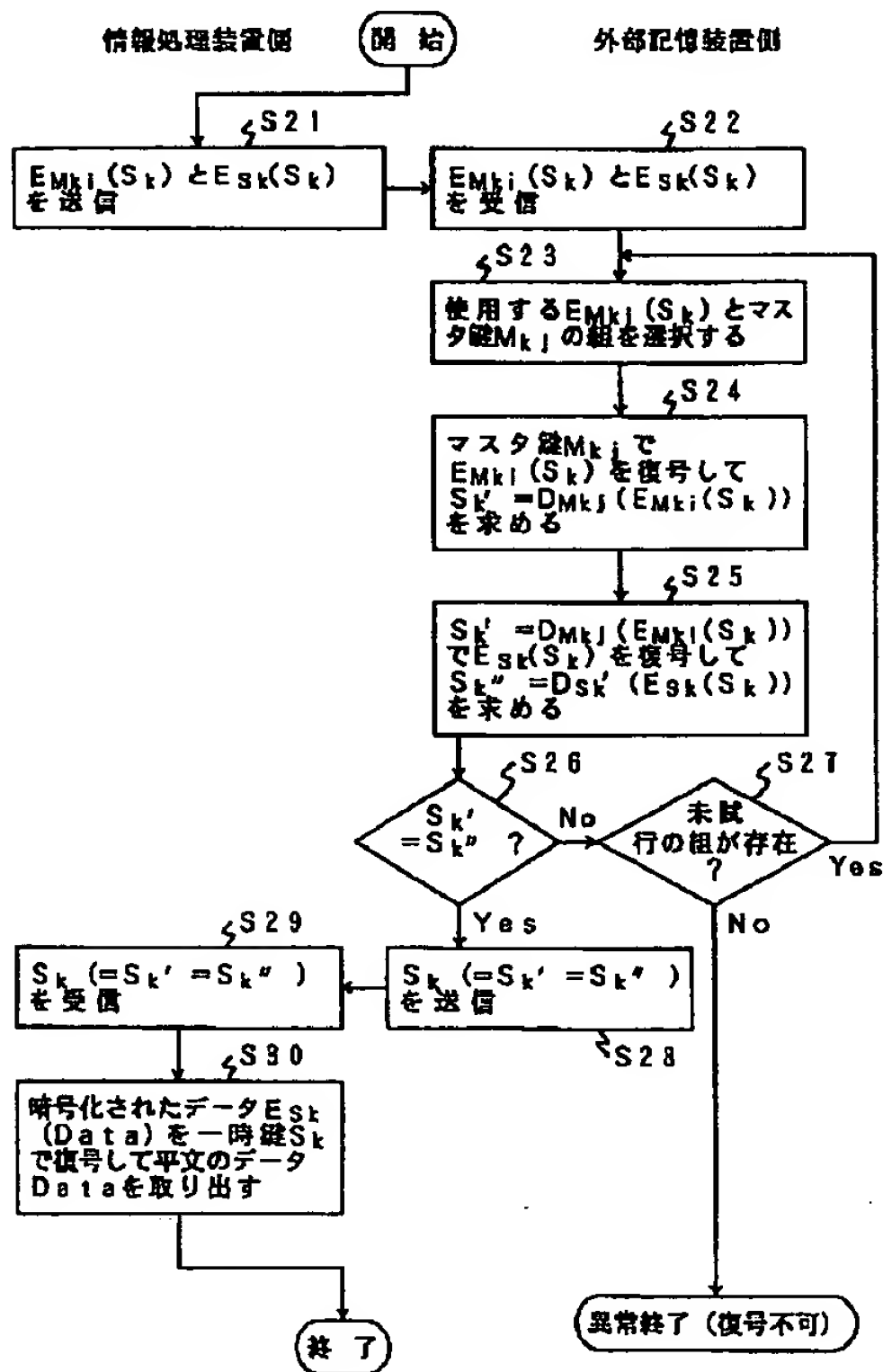
【図14】



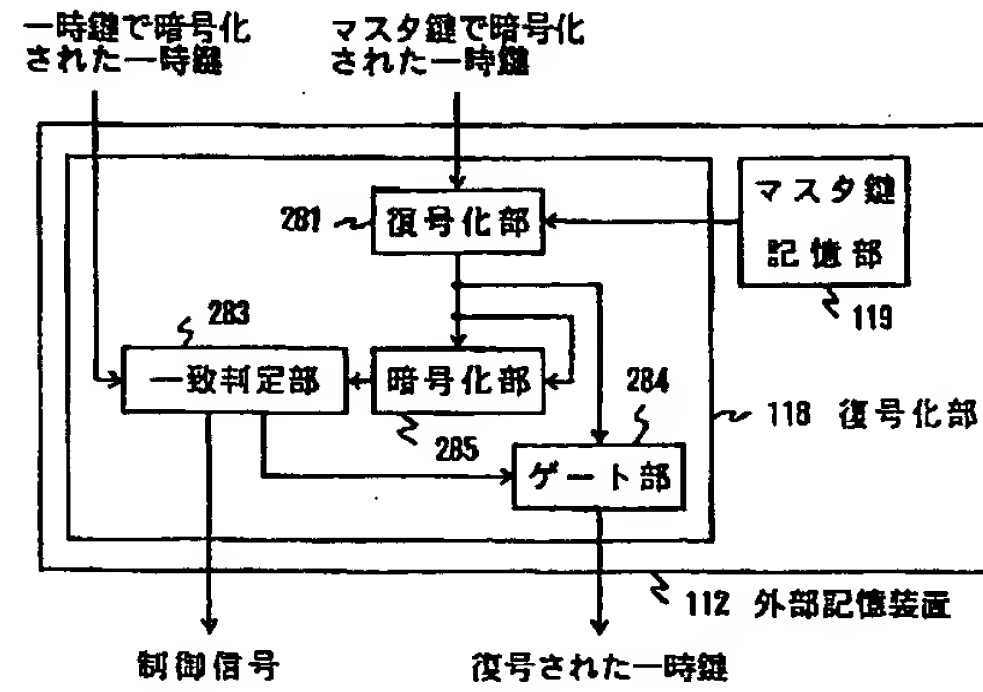
【図15】



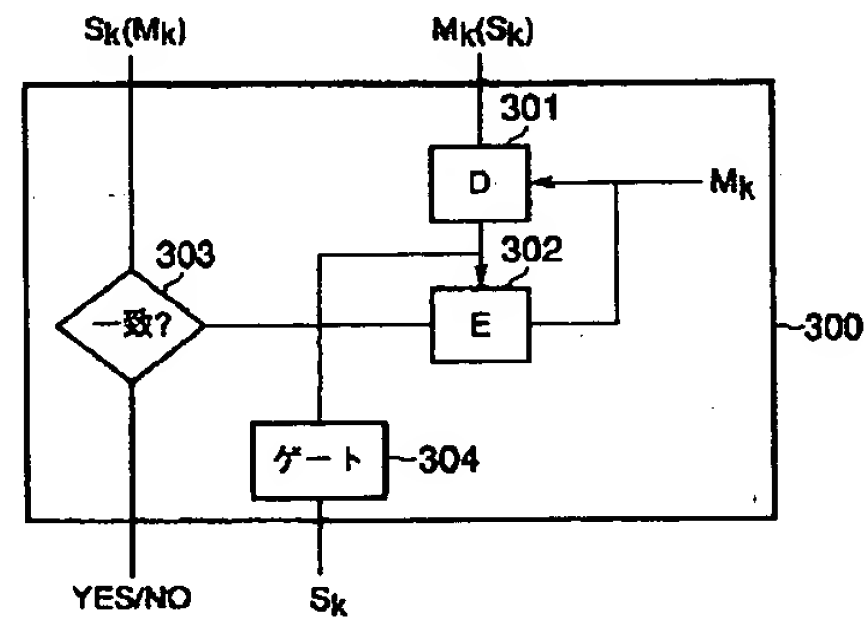
【図16】



【図17】



【図20】

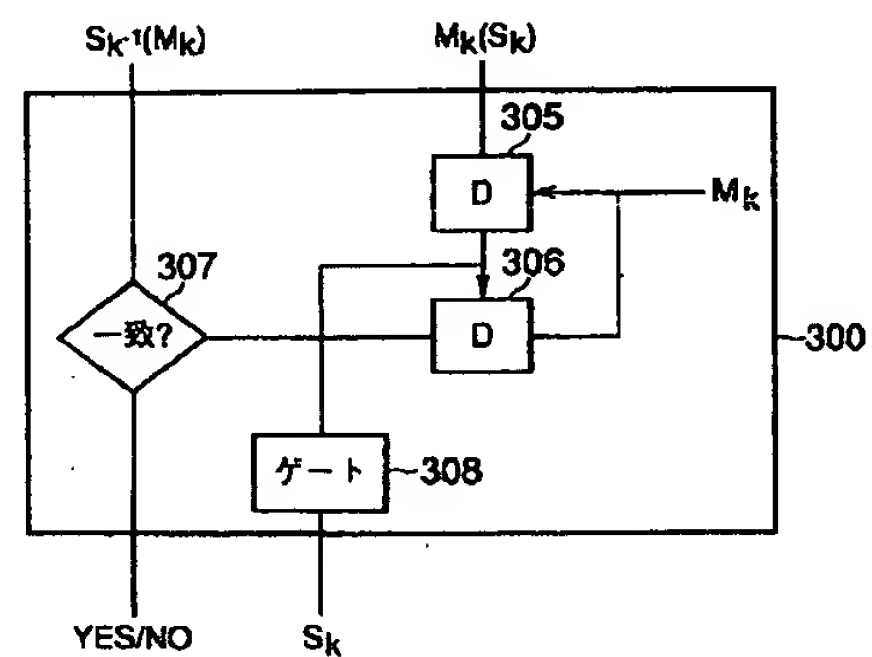


【図19】

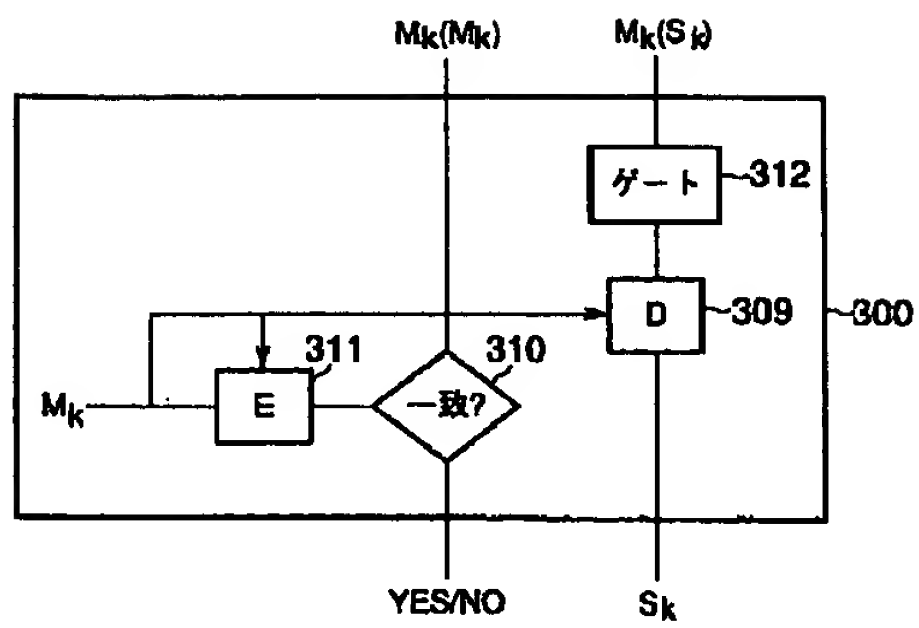
鍵チェック方式 チェック関数

	Mkの暗号化/復号		Skの暗号化/復号	
	含む	含まない	含む	含まない
MkとSk	Sk(Mk) Sk'(Mk)	h(Mk Sk)	Mk'(Sk) Mk'(Sk)	h(Mk Sk)
Mkのみ/Mk と他のデータ	Mk(Mk) Mk'(Mk) Mk(Mk+d*) Mk'(Mk+d*)	Mk(d*) Mk'(d*) h(Mk)		
Skのみ/Skと 他のデータ			Sk(Sk) Sk'(Sk)	Sk(d) Sk'(d) h(Sk)

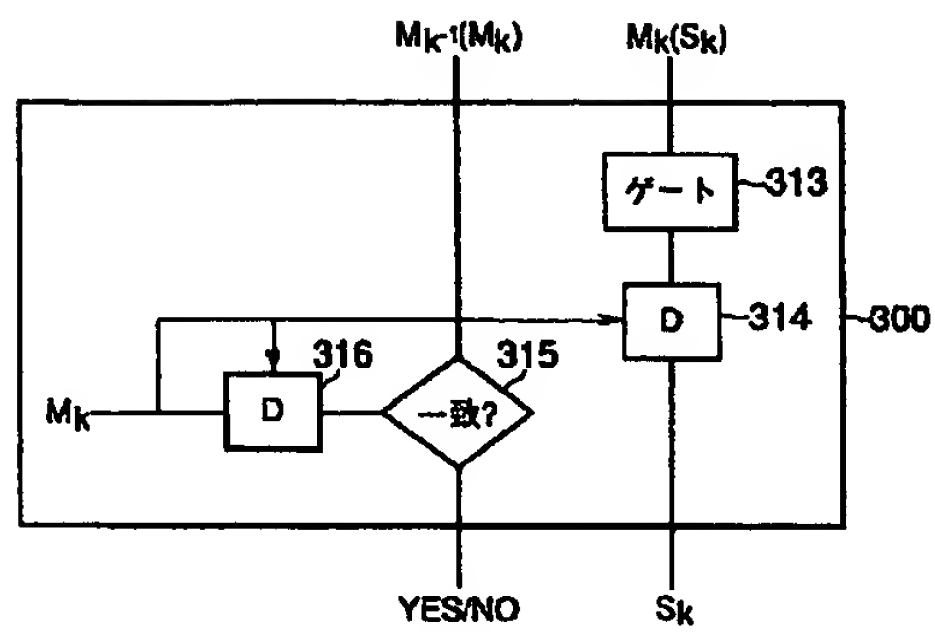
【図21】



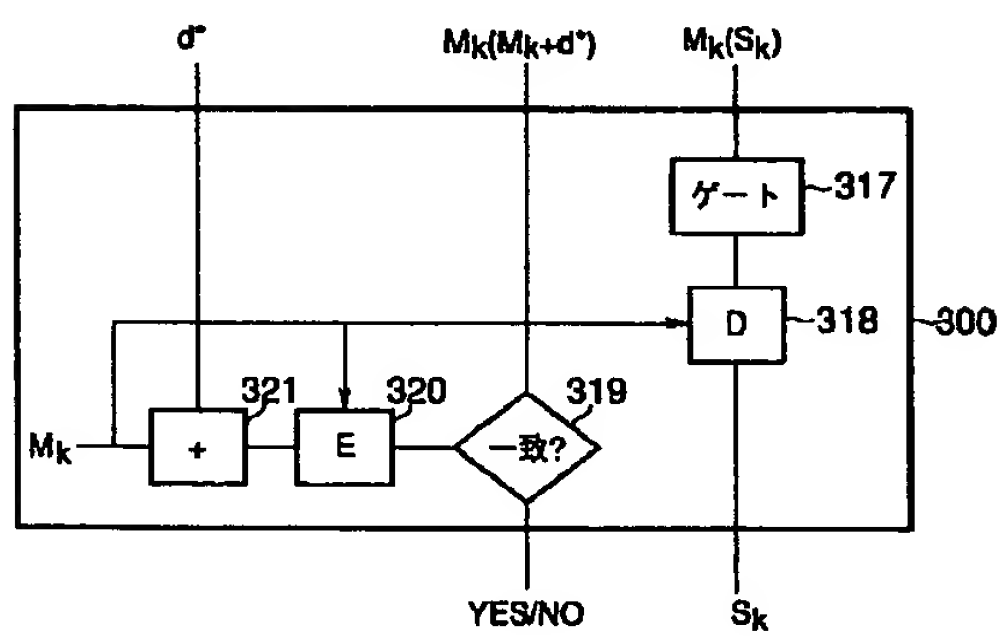
【図22】



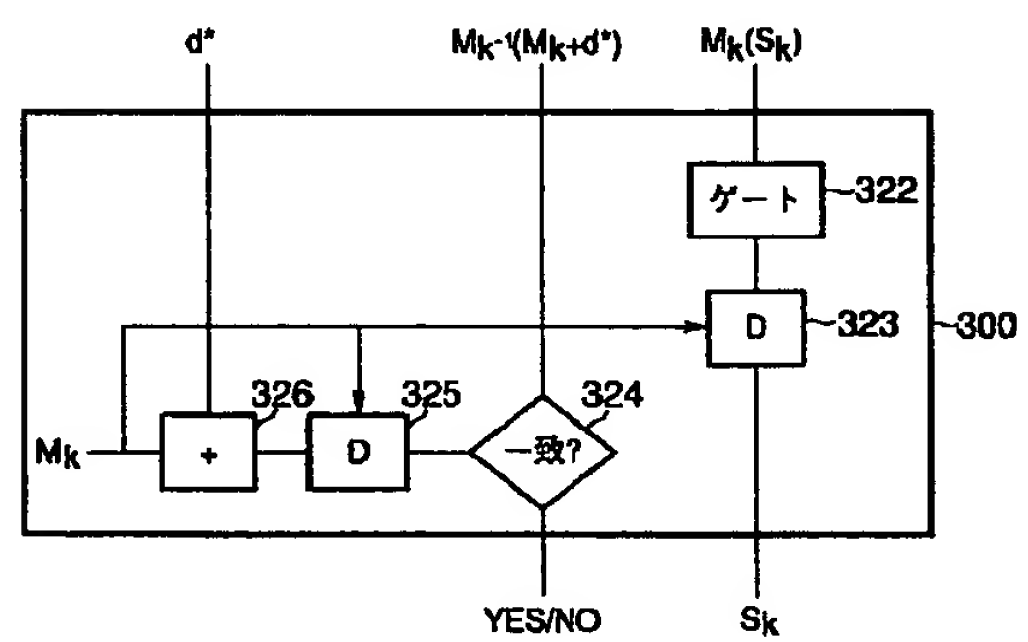
【図23】



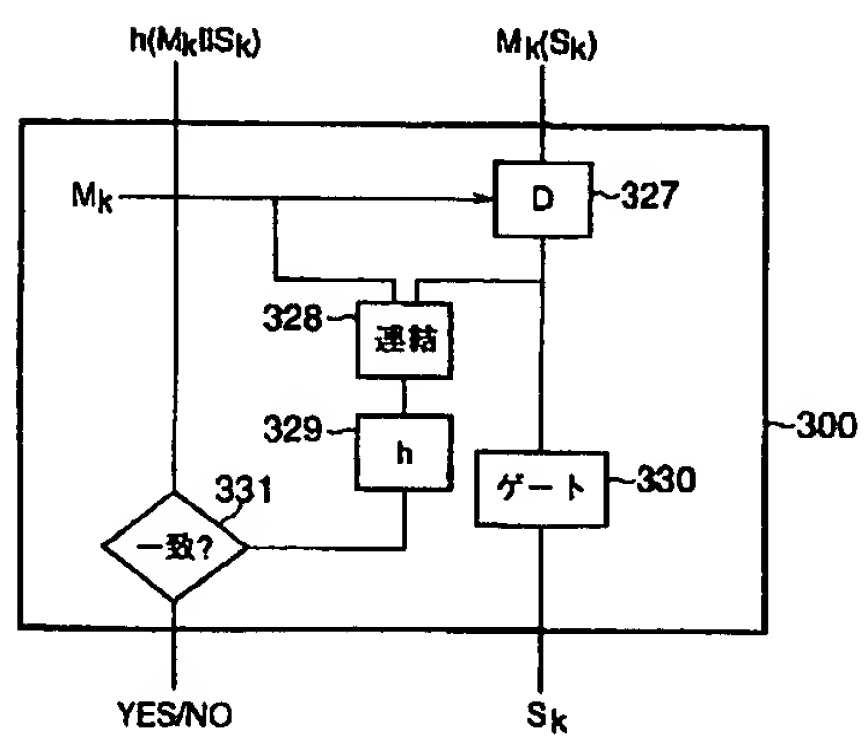
【図24】



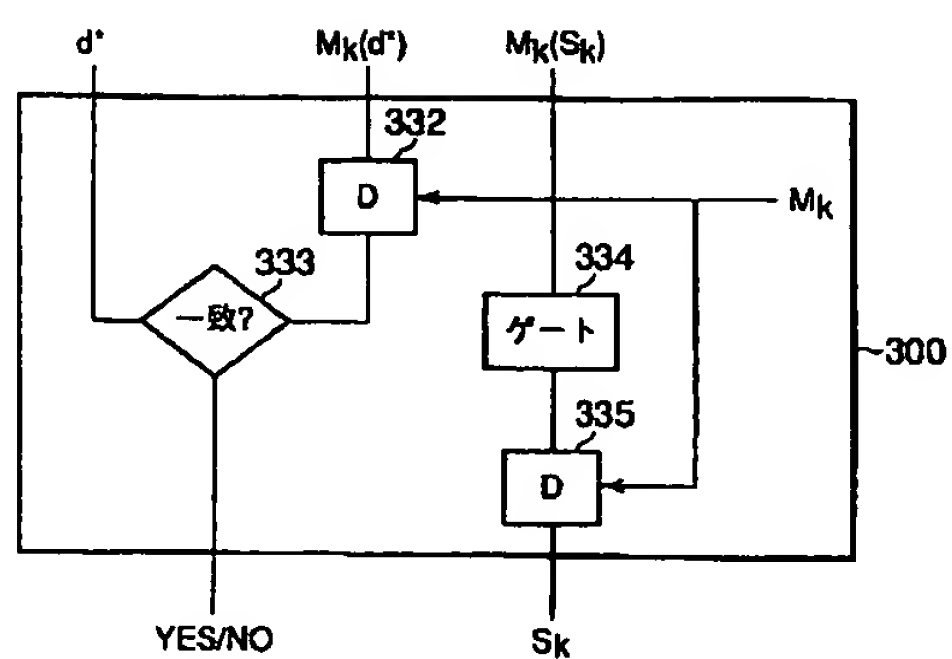
【図25】



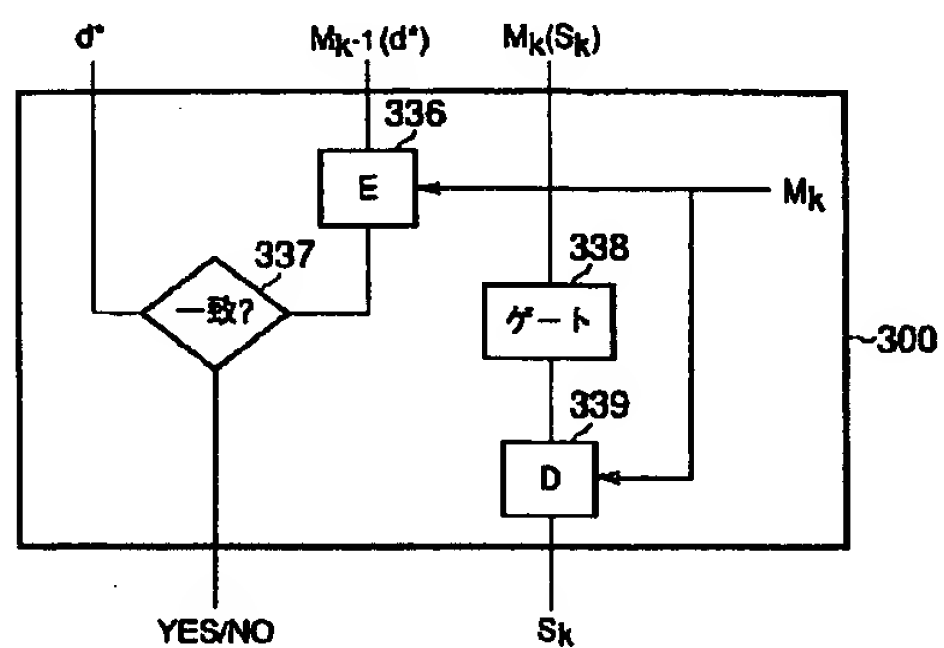
【図26】



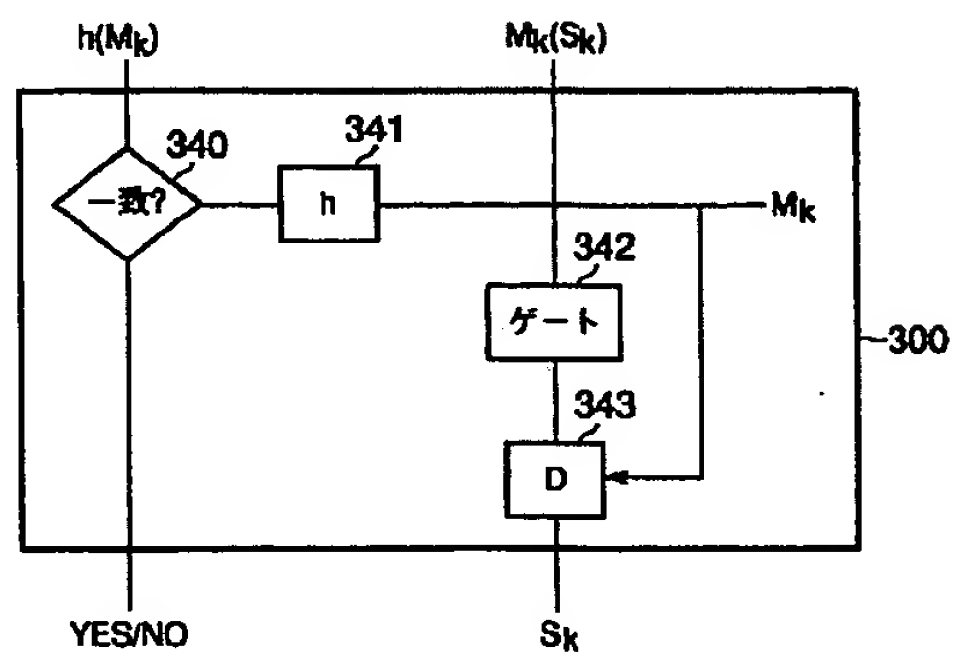
【図27】



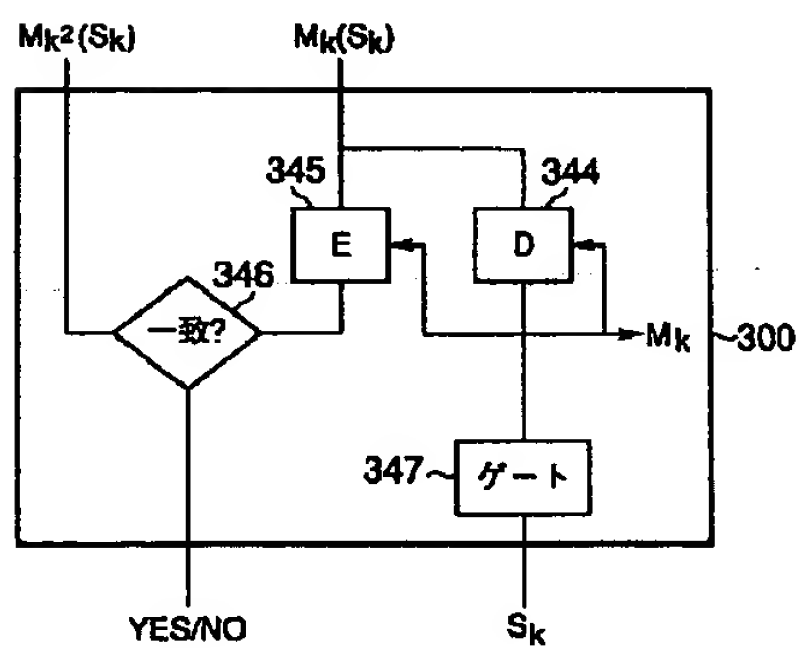
【図28】



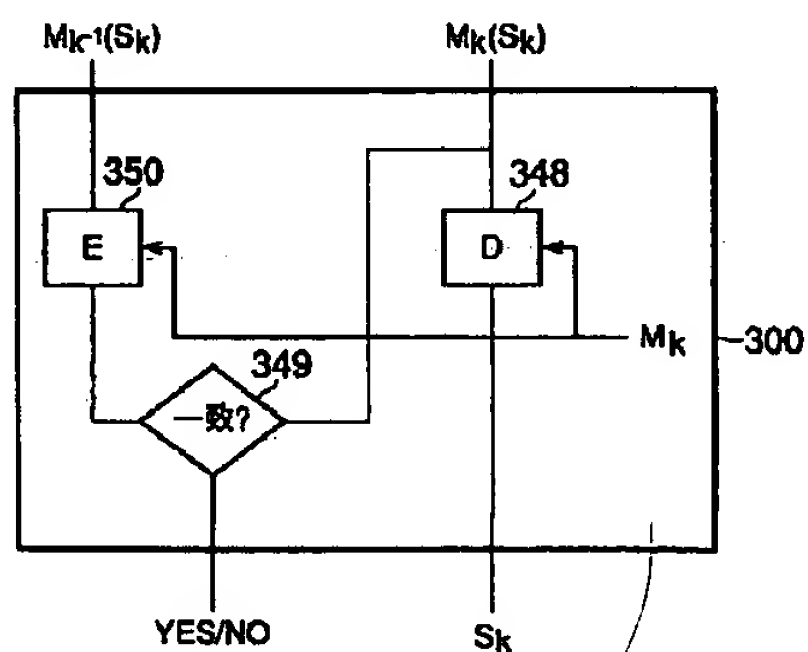
【図29】



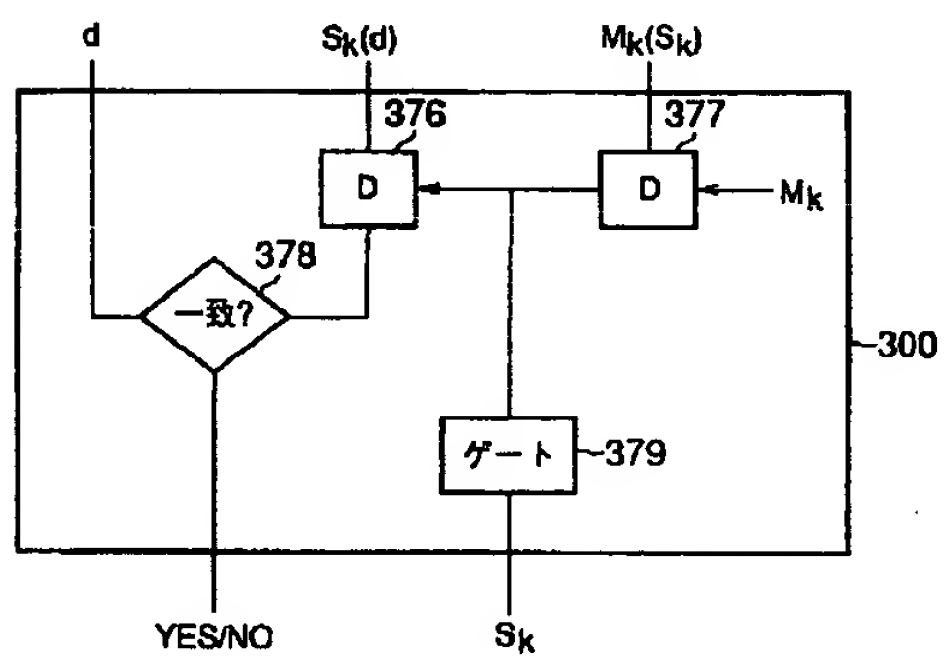
【図30】



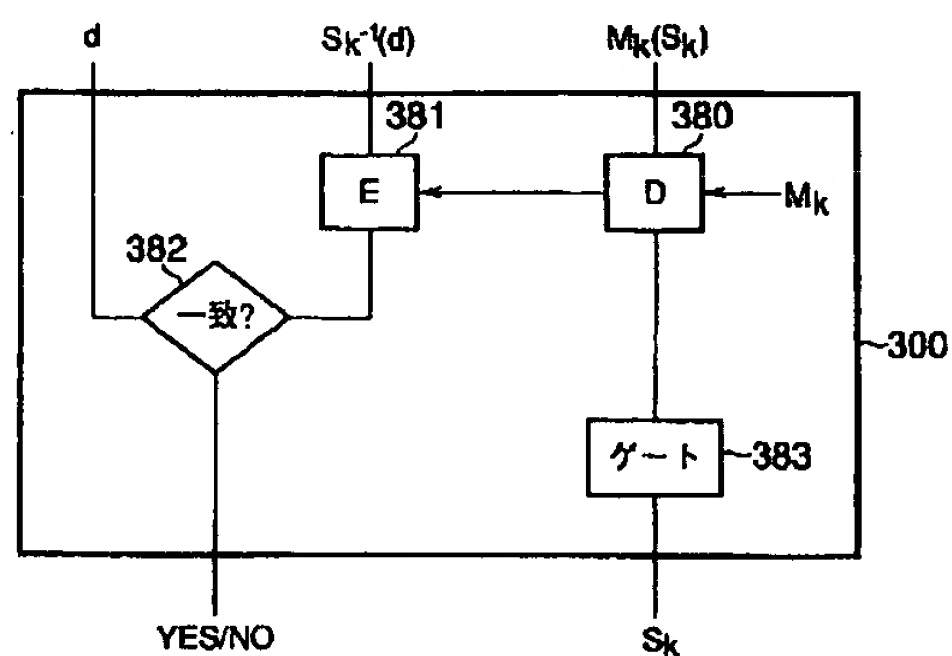
【図31】



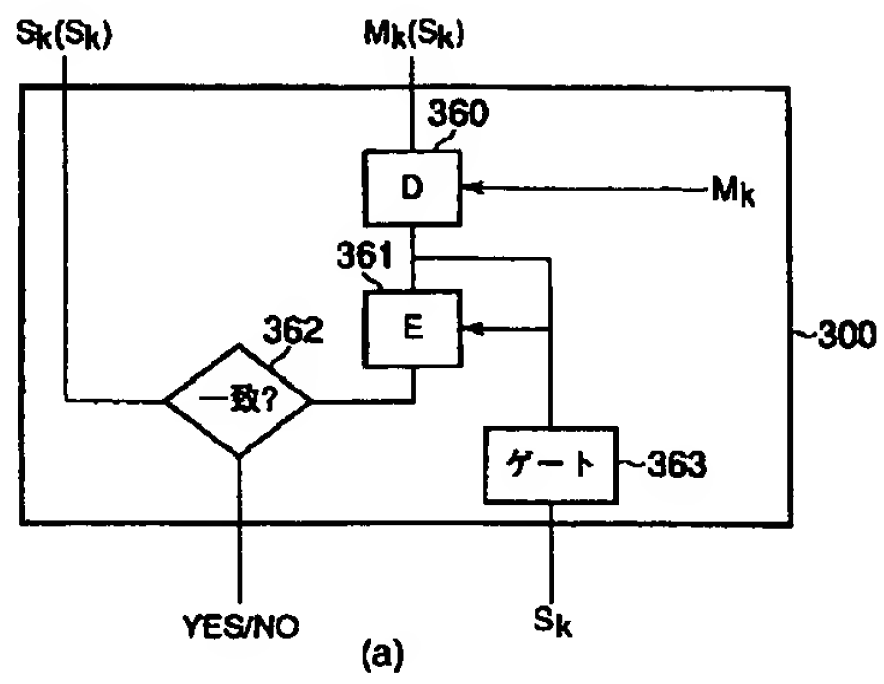
【図34】



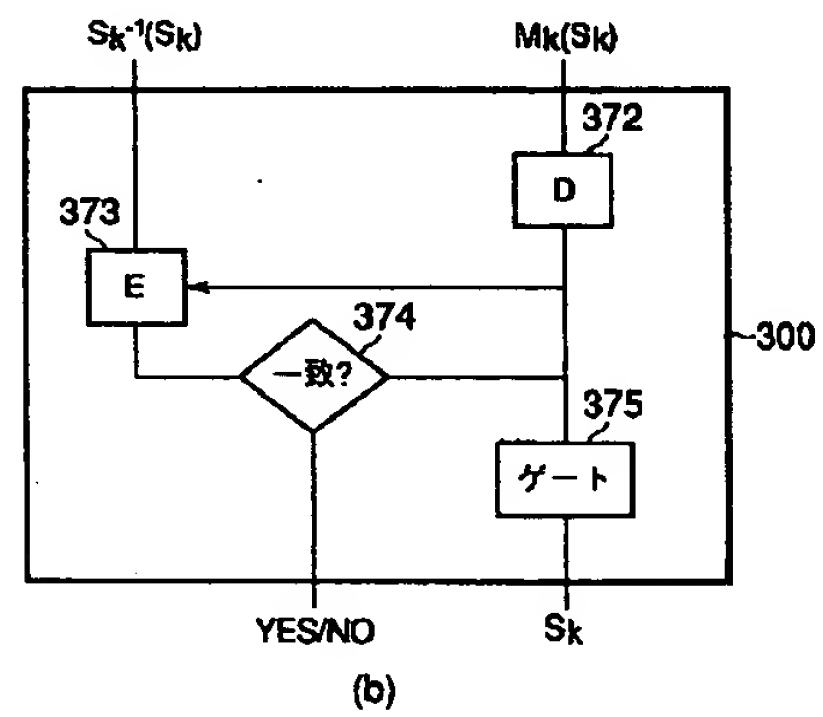
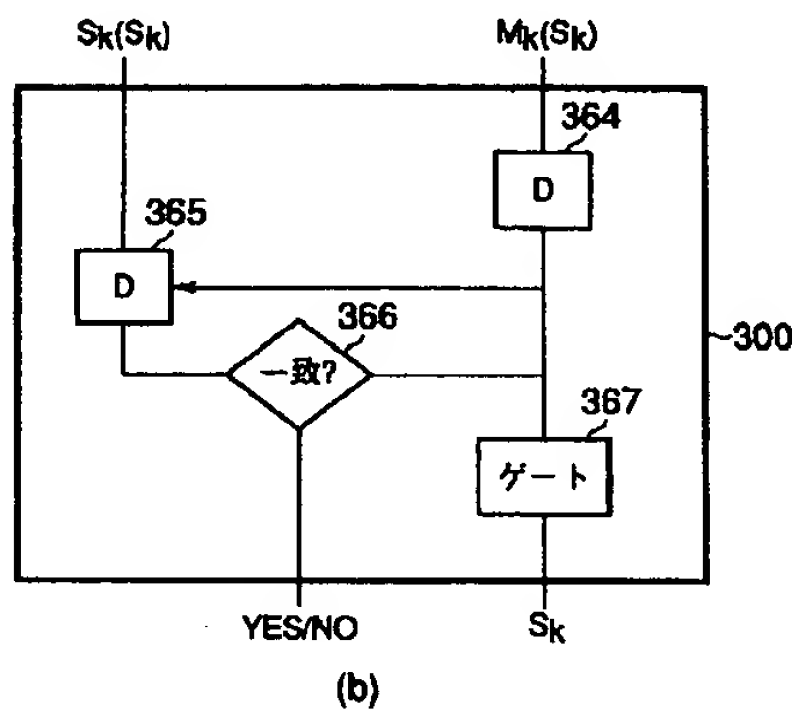
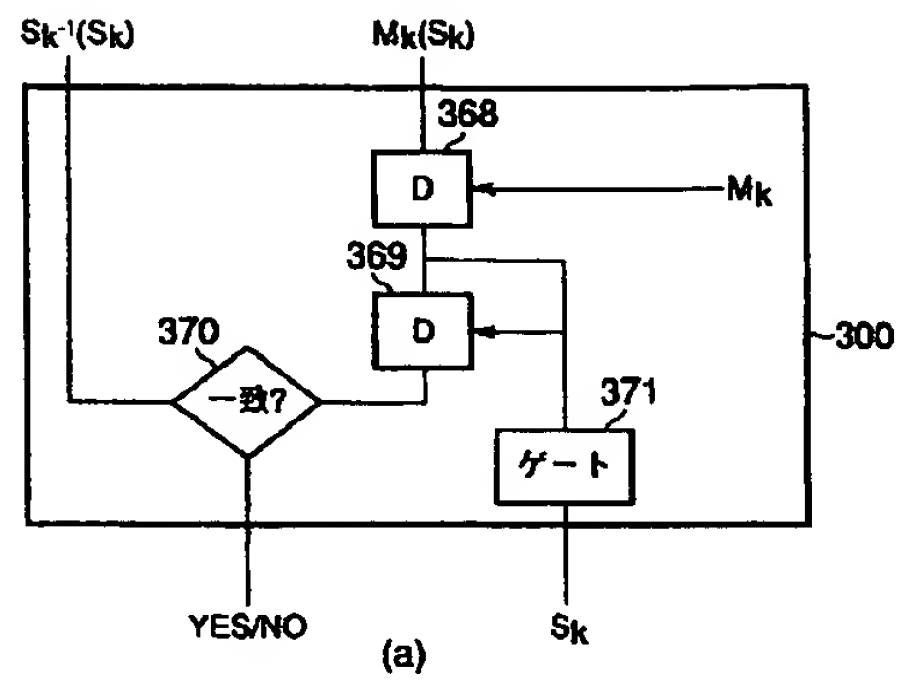
【図35】



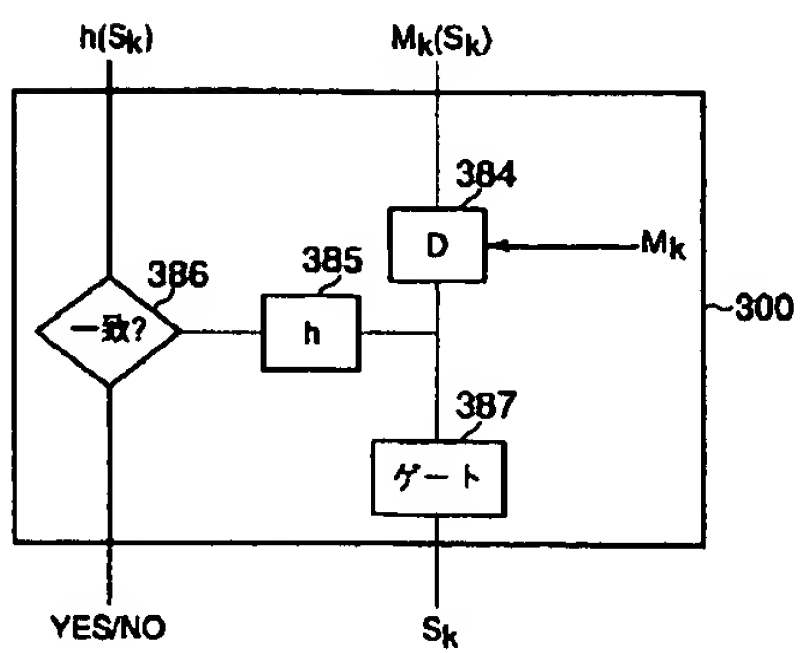
【図32】



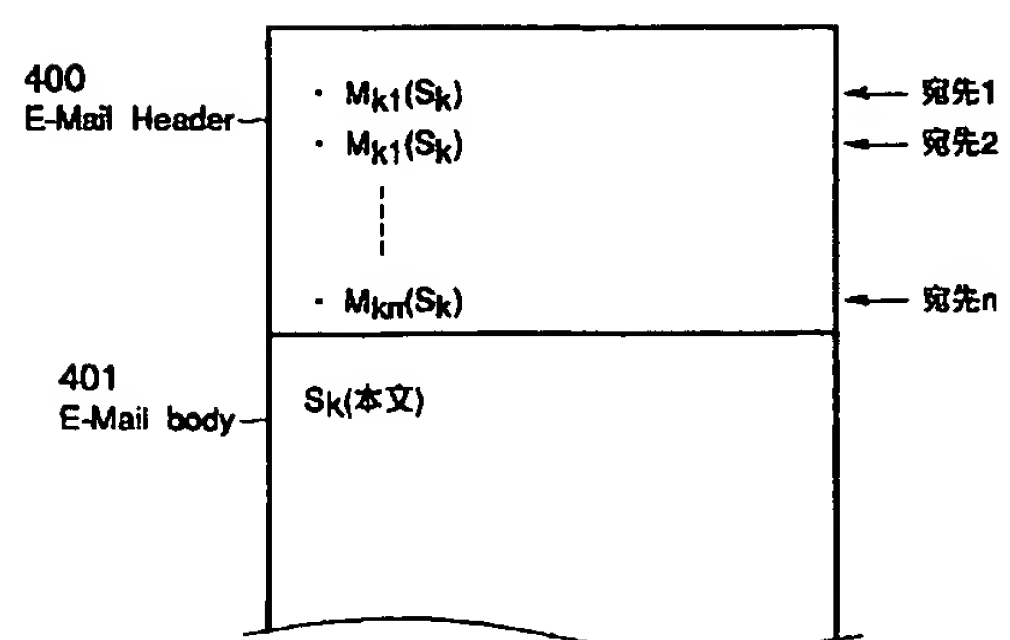
【図33】



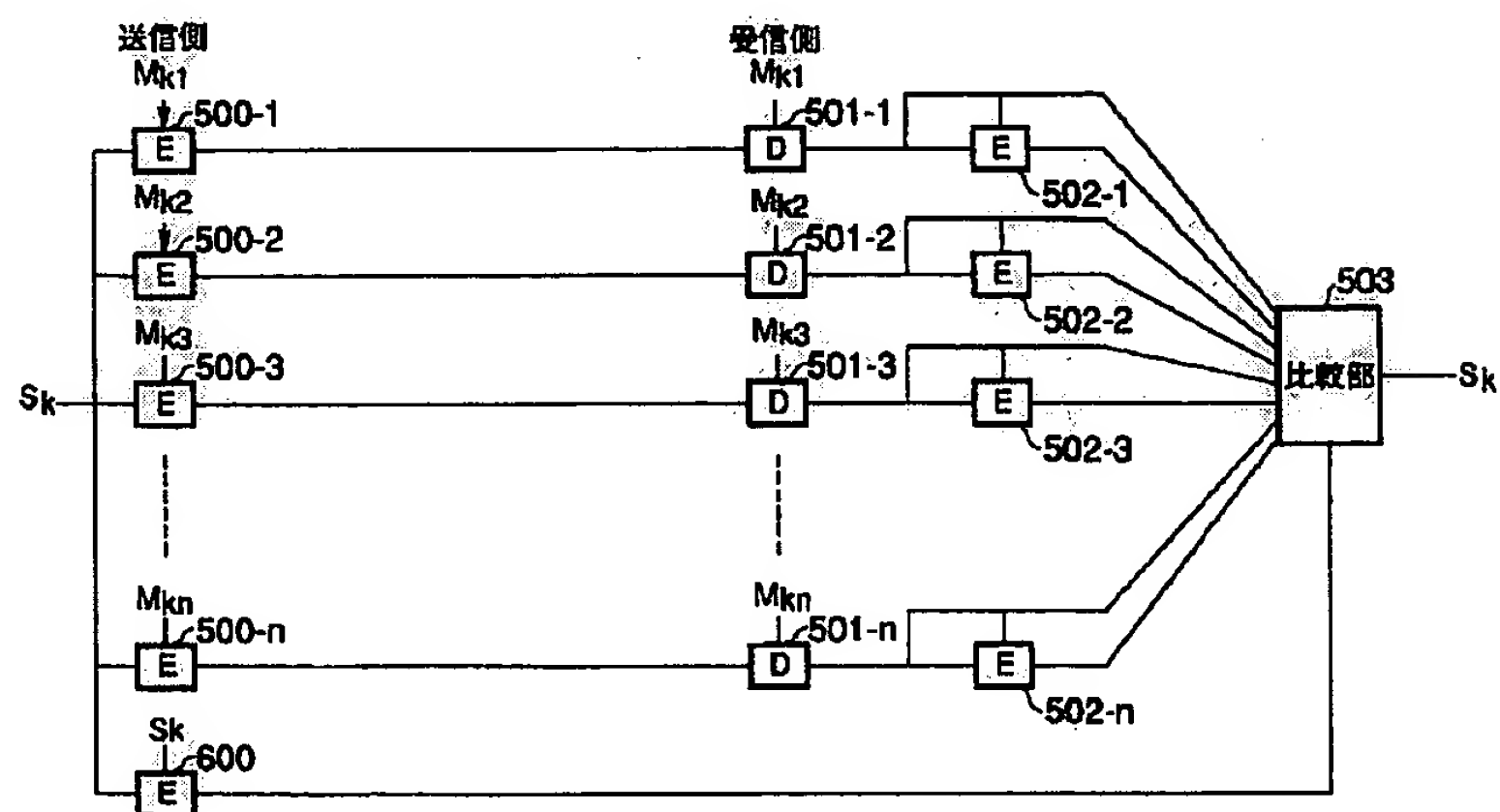
【図36】



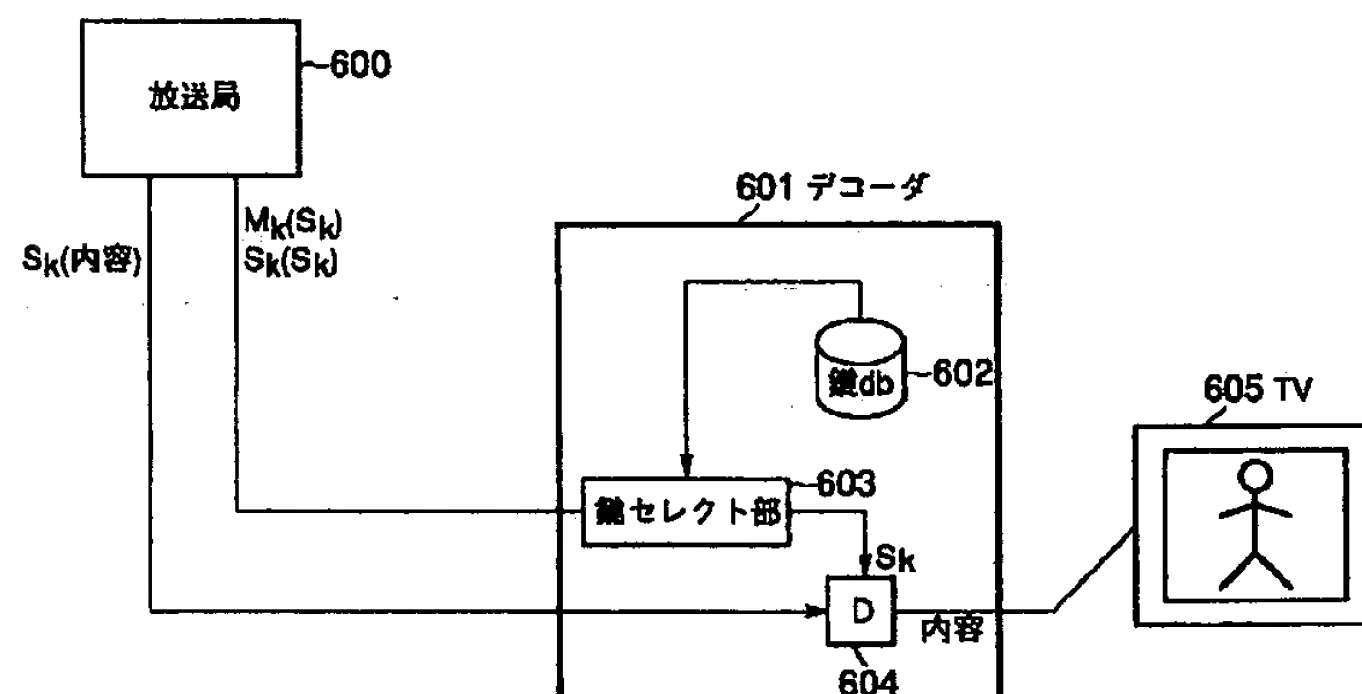
【図37】



【図38】



【図39】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 9/10

H 0 4 L 9/00

6 2 1 A

(72) 発明者 堀 智美

神奈川県川崎市幸区小向東芝町1番地 株
 式会社東芝研究開発センター内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)